

مكتب الأمم المتحدة المعني بالمخدرات والجريمة

دراسة شاملة
عن الجريمة السيبرانية

مسودة ـــ شباط/فبراير 2013

مكتب الأمم المتحدة المعني بالمخدرات والجريمة

فيينا

دراسة شاملة عن الجريمة السيبرانية

مسودة

شباط/فبراير 2013



الأمم المتحدة

نيويورك، 2013

ACKNOWLEDGEMENTS

This report was prepared for the open-ended intergovernmental expert group on cybercrime by Conference Support Section, Organized Crime Branch, Division for Treaty Affairs, UNODC, under the supervision of John Sandage (Director, Division for Treaty Affairs), Sara Greenblatt (Chief, Organized Crime Branch), and Gillian Murray (UNODC Senior Focal Point for Cybercrime and Chief, Conference Support Section).

Study team:

Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (UNODC)

Consultants:

Ulrich Sieber, Tatiana Tropina, Nicolas von zur Mühlen
(Max Planck Institute for Foreign and International Criminal Law)

Ian Brown, Joss Wright
(Oxford Internet Institute and Cyber Security Centre, University of Oxford)

Roderic Broadhurst
(Australian National University)

Kristin Krüger
(Brandenburg Institute for Society and Security)

المحتويات

قائمة الاختصارات

الاختصارات

CERT	فريق مواجهة الطوارئ الحاسوبية
CSIRT	فريق الاستجابة لحوادث أمن الفضاء الإلكتروني
ECHR	الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية
ECtHR	المحكمة الأوروبية لحقوق الإنسان
EU	الاتحاد الأوروبي
EUROPOL	مكتب الشرطة الأوروبي
G8	مجموعة الثماني
GDP	الناتج المحلي الاجمالي
HDI	دليل التنمية البشرية
ICCPR	العهد الدولي الخاص بالحقوق المدنية والسياسية
ICCPR-OP2	البروتوكول الاختياري الثاني الملحق بالعهد الدولي الخاص بالحقوق المدنية والسياسية، الذي يهدف إلى إلغاء عقوبة الإعدام
ICERD	الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري
ICESCR	العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية
ICRMW	الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم
ICT	تكنولوجيا المعلومات والاتصالات
INTERPOL	المنظمة الدولية للشرطة الجنائية
IP	بروتكولات الإنترنت
ISP	مقدمو خدمة الإنترنت
IT	تكنولوجيا المعلومات
ITU	الاتحاد الدولي للاتصالات
NFC	اتصالات المجال القريب
OP-CRC-SC	البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية
P2P	النظراء

SCO	منظمة شنغهاي للتعاون
SMS	خدمة الرسائل القصيرة
TRIPS	الاتفاق المتعلق بالجوانب المتصلة بالتجارة من حقوق الملكية الفكرية
UNESCO	منظمة الأمم المتحدة للتربية والعلم والثقافة
UNODC	مكتب الأمم المتحدة المعني بالمخدرات والجريمة
UNSC	مجلس الأمن التابع للأمم المتحدة
URL	الاسم التقني لعنوان الموقع الالكتروني على الإنترنت
USB	تسلسل الناقل العام
VGT	فريق العمل العالمية الافتراضية
WEF	المنتدى الاقتصادي العالمي

الاتحاد الأفريقي، 2012. مشروع اتفاقية بشأن إنشاء إطار قانوني للمساعدة في الأمن السيبراني في أفريقيا (**مشروع اتفاقية الاتحاد الأفريقي**).

السوق المشتركة لشرق وجنوب أفريقيا (كوميسا)، 2011. مشروع القانون النموذجي بشأن الأمن السيبراني. (**مشروع القانون النموذجي للكوميسا**).

الكومنولث 2002، (1) مشروع قانون الحاسوب والجرائم ذات الصلة بالحاسوب و(2) القانون النموذجي بشأن الأدلة الإلكترونية (**القانون النموذجي لدول اتحاد الكومنولث**).

كومنولث الدول المستقلة، 2001. اتفاقية بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية (**اتفاقية كومنولث الدول المستقلة**).

مجلس أوروبا، 2001. اتفاقية بشأن الجريمة السيبرانية والبرتوكول الإضافي للاتفاقية بشأن الجريمة السيبرانية، المعني بتجريم أفعال ذات طبيعة عنصرية أو كراهية الأجانب المرتكبة بواسطة النظم الحاسوبية (**اتفاقية/بروتوكول مجلس أوروبا بشأن الجريمة السيبرانية**).

مجلس أوروبا، 2007. اتفاقية حماية الأطفال ضد الاستغلال الجنسي والاعتداء الجنسي (**اتفاقية مجلس أوروبا لحماية الطفل**).

الجماعة الاقتصادية لدول غرب أفريقيا (ايكواس)، 2009. مشروع توجيهي بشأن مكافحة الجريمة السيبرانية داخل دول غرب أفريقيا (**المشروع التوجيهي للايكواس**).

الاتحاد الأوروبي، 2000. التوجيه 2000/31/EC الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الجوانب القانونية المحدِدة لخدمات مجتمع المعلومات، لاسيما التجارة الإلكترونية، في السوق الداخلي (**التوجيه الأوروبي بشأن التجارة الإلكترونية**).

الاتحاد الأوروبي، 2001. القرار الإطاري للمجلس الأوروبي 2001/413/JHA لمكافحة الاحتيال والتزوير في وسائط الدفع غير النقدية (**قرار الاتحاد الأوروبي بشأن الاحتيال والتزوير**).

الاتحاد الأوروبي، 2002. التوجيه 2002/58/EC الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية (**توجيه الاتحاد الأوروبي بشأن حماية البيانات**).

الاتحاد الأوروبي، 2005. القرار الإطاري للمجلس 2005/222/JHA بشأن الهجمات ضد نظم المعلومات (**قرار الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات**).

الاتحاد الأوروبي، 2006. التوجيه 2006/24/EC الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الاحتفاظ بالبيانات التي تم إنشاؤها أو معالجتها فيما يتعلق بتوفير خدمات الاتصالات الإلكترونية المتاحة للجمهور أو شبكات الاتصالات العامة (**توجيه الاتحاد الأوروبي بشأن الإبقاء على البيانات**).

الاتحاد الأوروبي، 2010. المشروع COM(2010) 517 النهائي التوجيهي للبرلمان الأوروبي ومجلس أوروبا بشأن الهجمات ضد نظم المعلومات واستبدال القرار الإطاري للمجلس 2005/222/JHA. (**المشروع التوجيهي للاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات**).

الاتحاد الأوروبي، 2011. التوجيه 2011/92/EU للبرلمان الأوروبي ومجلس أوروبا بشأن مكافحة الاعتداء الجنسي والاستغلال الجنسي للأطفال واستغلال الأطفال في المواد الإباحية، واستبدال القرار الإطاري للمجلس 2004/68/JHA (**توجيه الاتحاد الأوروبي بشأن استغلال الأطفال**).

الاتحاد الدولي للاتصالات (ITU)/الجماعة الكاريبية (CARICOM)/الاتحاد الكاريبي للاتصالات (CTU)، 2010. النصوص التشريعية النموذجية بشأن الجريمة السيبرانية/الجرائم الإلكترونية والأدلة الإلكترونية (**الاتحاد الدولي للاتصالات/الجماعة الكاريبية/النصوص التشريعية النموذجية للاتحاد الكاريبي للاتصالات**).

جامعة الدول العربية، 2010. الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات (**اتفاقية جامعة الدول العربية**).

جامعة الدول العربية، 2004. القانون العربي النموذجي لمكافحة الجرائم المتعلقة بنظم تكنولوجيا المعلومات. (**القانون النموذجي لجامعة الدول العربية**)

منظمة شنغهاي للتعاون، 2010. اتفاقية التعاون في مجال أمن المعلومات الدولية (**اتفاقية منظمة شنغهاي للتعاون**).

الأمم المتحدة، 2000. البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال وبغاء الأطفال واستغلال الأطفال في المواد الإباحية (**الأمم المتحدة – البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال وبغاء الأطفال واستغلال الأطفال في المواد الإباحية OP-CRC-SC**).

مقدمة

طلبت الجمعية العامة، في قرارها 230/65، إلى لجنة منع الجريمة والعدالة الجنائية أن تنشئ فريقَ خبراء حكوميٍّ دولي مفتوح العضوية، من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبرانية، وللتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية، وأفضل الممارسات، والمساعدة الفنية والتعاون الدولي.

طلبت الجمعية العامة، في قرارها 230/65، إلى لجنة منع الجريمة والعدالة الجنائية أن تنشئ، وفقا للفقرة 42 من إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نُظُم منع الجريمة والعدالة الجنائية وتطورها في عالم متغيّر، فريقَ خبراء حكومي دولي مفتوح العضوية من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبرانية وللتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، بما في ذلك تبادل المعلومات عن التشريعات الوطنية وأفضل الممارسات والمساعدة الفنية والتعاون الدولي، بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجرائم السيبرانية واقتراح تدابير جديدة في هذا الشأن.[1]

أحاطت الجمعية العامة علما مع التقدير، في قرارها 189/67، بعمل فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية، وشجّعته على تحسين الجهود التي يبذلها من أجل إنجاز أعماله وعرض نتائج الدراسة في الوقت المناسب على لجنة منع الجريمة والعدالة الجنائية.

وقد عُقدت الدورة الأولى لفريق الخبراء في فيينا في الفترة الممتدة من 17 إلى 21 كانون الثاني/يناير 2011، وقام خلالها فريق الخبراء باستعراض واعتماد مجموعة من المواضيع وكذلك منهجية للدراسة.[2]

تضمنت مجموعة المواضيع المطروحة للنظر فيها ضمن إطار الدراسة الشاملة للجريمة السيبرانية، مشكلة الجريمة السيبرانية، وتدابير التصدّي القانونية للجريمة السيبرانية، وقدرات منع الجريمة والعدالة الجنائية وتدابير التصدّي الأخرى للجريمة السيبرانية، والمنظمات الدولية، والمساعدة الفنية. ثم قسمت هذه الموضوعات إلى 12 موضوعا فرعيا.[3] وتم تناول هذه الموضوعات في سياق هذه الدراسة في ثمانية فصول: (1) الموصولية والجريمة السيبرانية؛ (2) الصورة العالمية؛ (3) التشريعات والأطر؛ (4) التجريم؛ (5) السلطات المعنية بإنفاذ

[1] مرفق قرار الجمعية العامة 230/65.

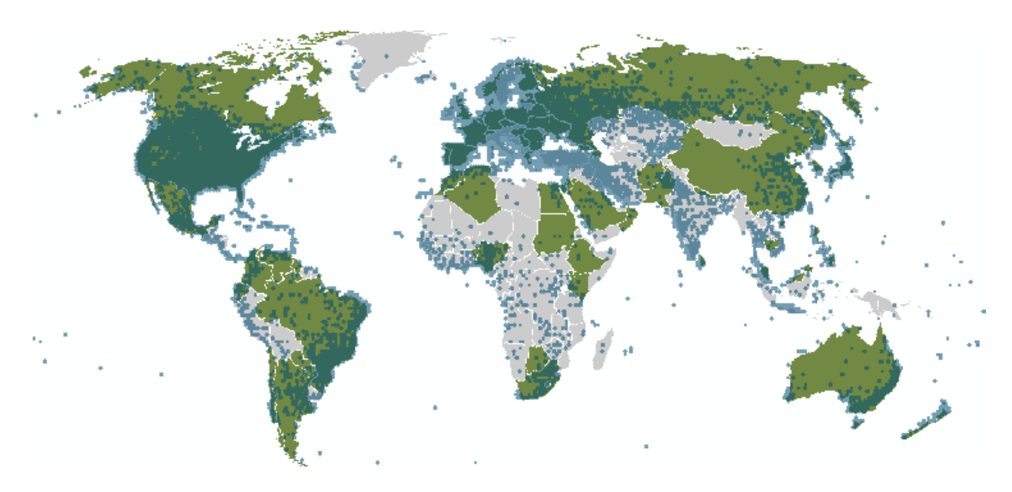
[2] E/CN.15/2011/19.

[3] (1) ظاهرة الجريمة السيبرانية؛ (2) معلومات إحصائية؛ (3) تحديات الجريمة السيبرانية؛ (4) المناهج المشتركة للتشريعات؛ (5) التجريم؛ (6) الصلاحيات الإجرائية؛ (7) التعاون الدولي؛ (8) الأدلة الإلكترونية؛ (9) أدوار ومسؤوليات مقدّمي الخدمات والقطاع الخاص؛ (10) قدرات منع الجريمة والعدالة الجنائية وتدابير التصدّي الأخرى للجريمة السيبرانية؛ (11) المنظمات الدولية؛ (12) المساعدة الفنية.

القانون والتحقيقات؛ (6) الأدلة الإلكترونية والتدابير المتخذة في مجال العدالة الجنائية؛ (7) التعاون الدولي؛ و(8) منع الجريمة السيبرانية.

وفي إطار منهجية الدراسة؛ كُلّف مكتب الأمم المتحدة المعني بالمخدرات والجريمة بإعداد الدراسة، بما في ذلك إعداد استبيان بهدف جمع المعلومات، وجمع البيانات وتحليلها، وإعداد مشروع لنص الدراسة. وتقرَّر في إطار جمع المعلومات وفقا لمنهجية الدراسة التي أعدها مكتب الأمم المتحدة المعني بالمخدرات والجريمة، توزيع استبيان على الدول الأعضاء والمنظمات الحكومية الدولية وممثلين عن القطاع الخاص والمؤسسات الأكاديمية من شهر شباط/فبراير 2012 إلى شهر تموز/يوليو 2012. وقد وردت إلى مكتب الأمم المتحدة المعني بالمخدرات والجريمة معلومات من 69 دولة عضوا، فيما يلي توزيعها الإقليمي: أفريقيا (11)، والأمريكتين (13)، وآسيا (19)، وأوروبا (24)، وأوقيانوسيا (2). واستُلمت المعلومات من 40 منظّمة من القطاع الخاص و16 منظّمة أكاديمية و11 منظمة حكومية دولية. واستعرضت الأمانة أيضا أكثر من 500 وثيقة من مصادر مفتوحة. ويتضمن الملحق الخامس بهذه الدراسة مزيدا من التفاصيل بشأن المنهجية.

ردود الدول الأعضاء على الاستبيان الخاص بالدراسة (الأخضر)وانتشار الإنترنت (الأزرق)



المصدر: الردود الخاصة بالاستبيان، إعداد مكتب الأمم المتحدة المعني بالمخدرات والجريمة GeoCityLite MaxMind

ووفقا لقرار الجمعية العامة 230/65، تم إعداد هذه الدراسة بغية "اختبار الخيارات المتاحة لتعزيز التدابير القانونية أو غيرها من التدابير القائمة على الصعيدين الوطني والدولي للتصدي للجرائم السيبرانية واقتراح تدابير جديدة في هذا الشأن." ويأتي التكليف في سياق عدد من التكليفات، وغيرها من الأنشطة المتعلقة بالجريمة السيبرانية والأمن السيبراني داخل منظومة الأمم المتحدة.[1] وفي هذا الصدد، اقتصر تركيز الدراسة على جوانب منع *الجريمة* و*العدالة الجنائية* في إطار منع الجريمة السيبرانية ومكافحتها.

[1] بما في ذلك العمل في سياق التطورات التي يشهدها مجال المعلومات والاتصالات في سياق الأمن الدولي. انظر A/RES/66/24

وتمثل هذه الدراسة "استعراضا سريعا" في الوقت المناسب لجهود العدالة الجنائية والوقاية من الجريمة لمكافحة الجريمة السيبرانية ومنعها.

إن هذه الدراسة ترسم صورة عالمية، وتسلط الضوء على الدروس المستفادة من الجهود المبذولة الحالية والسابقة، كما تقدم خيارات ممكنة للاستجابة في المستقبل. ورغم أن هذه الدراسة تدور حول "الجريمة السيبرانية"، كما ينصّ عنوانها، إلا أنها ذات أهمية منقطعة النظير لجميع الجرائم. ومع انتقال العالم إلى مجتمع يتسم بالموصولية البالغة، أصبح من الصعب تصوُّر وقوع "جريمة حاسوبية" وربما أيِّ جريمة أخرى لا تنطوي على أدلة إلكترونية تتعلق بالموصولية. وفي ضوء ذلك، فإن هذه التطورات تتطلب تغييرات جوهرية في طريقة إنفاذ القانون وجمع الأدلة وآليات التعاون الدولي في المسائل الجنائية.

الاستنتاجات الرئيسية والخيارات

طلبت الجمعية العامة، في قرارها 230/65، من فريق الخبراء الحكومي الدولي إعداد دراسة شاملة لمشكلة الجريمة السيبرانية بغية دراسة الخيارات المتاحة لتعزيز التدابير القانونية واقتراح تدابير قانونية أو تدابير أخرى جديدة وطنية ودولية للتصدي للجرائم السيبرانية. ويطرح هذا الجزء النتائج الرئيسية لهذه الدراسة، بالإضافة إلى الخيارات المتاحة.

الاستنتاجات الرئيسية

- **الاستنتاجات الرئيسية للدراسة تتعلق بقضايا:**
  - تأثير عدم اتساق الإجراءات على الصعيد الدولي وتنوّع القوانين المحلية المتعلقة بالجريمة السيبرانية على التعاون الدولي
  - الاعتماد على الوسائل التقليدية للتعاون الدولي الرسمي في المسائل الجنائية التي تنطوي على جرائم الإنترنت والأدلة السيبرانية لجميع الجرائم
  - دور "موقع" الأدلة
  - تنسيق الأطر القانونية الوطنية
  - سلطات إنفاذ القانون وقدرات العدالة الجنائية
  - أنشطة منع الجريمة السيبرانية

تناولت الدراسة مشكلة الجريمة السيبرانية من خلال منظور الحكومات، والقطاع الخاص، والأوساط الأكاديمية، والمنظمات الدولية، وقد تم طرح النتائج في ثمانية فصول تناولت الموصولية الخاصة بشبكة الإنترنت والجريمة السيبرانية، والصورة العالمية للجريمة السيبرانية، وأطر وتشريعات مكافحة الجريمة السيبرانية، وتجريم الجريمة السيبرانية، وإنفاذ القانون والتحقيقات في الجريمة السيبرانية، والأدلة الإلكترونية والعدالة الجنائية، والتعاون الدولي في المسائل الجنائية التي تنطوي على جريمة سيبرانية، والوقاية الجريمة السيبرانية.

وفيما يلي الاستنتاجات الرئيسية في هذه المجالات، مع مزيد من التوضيح والتفصيل في الموجز التنفيذي الذي يلي هذا الجزء:

(أ) إنَّ التشظي الذي يطبع الساحة الدولية، وتنوّع القوانين المحلية المتعلقة بالجرايمة السيبرانية، قد يعزيان إلى وجود صكوك متعددة ذات نطاق موضوعي وجغرافي مختلف. وبينما تجسّد الصكوك شرعيًا الاختلافات الاجتماعية والثقافية والإقليمية القائمة، فإنَّ التباين في نطاق الصلاحيات الإجرائية

والأحكام المتعلقة بالتعاون الدولي قد يفضي إلى نشوء "مجموعات" تعاون من البلدان، مما لا يتناسب دائما مع الطبيعة العالمية للجريمة السيبرانية؛

(ب) إنَّ الاعتماد على الوسائل التقليدية للتعاون الدولي الرسمي في مسائل الجريمة السيبرانية لا يكفي حاليا للاستجابة في الوقت المناسب لمقتضيات الحصول على أدلّة إلكترونية سريعة الزوال والتغيُّر. وبما أنَّ عددا متزايدا من الجرائم يشتمل على أدلّة إلكترونية توجد في أماكن جغرافية متعددة، سيشكّل ذلك مشكلة ليس فقط بشأن الجريمة السيبرانية، وإنما بشأن كل الجرائم عموما؛

(ج) في عالم الحوسبة السحابية ومراكز البيانات، يجب إعادة تحديد مفهوم دور "موقع" الدليل، لأهداف منها التوصُّل إلى توافق في الآراء بشأن المسائل المتعلقة بوصول سلطات إنفاذ القانون مباشرة إلى المعلومات الموجودة خارج نطاق ولايتها القضائية؛

(د) إنَّ تحليل الأطر القانونية الوطنية المتوافرة يشير إلى عدم كفاية التنسيق فيما يتعلق بالجريمة السيبرانية "الأساسية"، وصلاحيات التحقيق، ومقبولية الدليل الإلكتروني. ويمثّل القانون الدولي لحقوق الإنسان مرجعا خارجيا هاما فيما يتعلق بمسائل التجريم والأحكام الإجرائية؛

(هـ) إنَّ سلطات إنفاذ القانون، والمدّعين العامين، والسلطات القضائية في البلدان النامية، تحتاج إلى دعم ومساعدة تِقنيين شاملين، على نحو مستدام، وعلى المدى البعيد، من أجل التحقيق في الجريمة السيبرانية ومكافحتها؛

(و) إنَّ أنشطة منع الجريمة السيبرانية في جميع البلدان تتطلب تعزيز الشراكات بين القطاعين العام والخاص، وإدماج الاستراتيجيات الخاصة بالجريمة السيبرانية ضمن منظور أوسع للأمن السيبراني، وذلك من خلال نهج كلي يشتمل على زيادة الوعي.

الخيارات المتاحة لتعزيز التدابير القانونية واقتراح تدابير قانونية أو تدابير أخرى جديدة وطنية ودولية للتصدي للجريمة السيبرانية

- تتضمن الخيارات المتاحة لتعزيز التدابير القانونية واقتراح تدابير قانونية أو تدابير أخرى جديدة وطنية ودولية للتصدي للجريمة السيبرانية:
  - صوغ أحكام نموذجية دولية
  - صوغ صك متعدد الأطراف بشأن التعاون الدولي فيما يتعلق بالأدلّة الإلكترونية في المسائل الجنائية
  - صوغ صك شامل متعدد الأطراف بشأن الجريمة السيبرانية
  - توفير مساعدة تقنية معزّزة للوقاية من الجريمة السيبرانية ومكافحتها في البلدان النامية

وقد استُمدت الخيارات المقدمة من ردود الدول على السؤال الذي ورد في الاستبيان الخاص بالدراسة بشأن الخيارات التي يتعين النظر فيها لتعزيز التدابير القانونية واقتراح تدابير قانونية أو تدابير أخرى جديدة وطنية ودولية للتصدي للجريمة السيبرانية، فضلا عن النتائج الرئيسية.

وفي مستعرض الإجابة على هذا السؤال، طرحت الدول مجموعة من الاحتمالات، حيث جاءت غالبية الخيارات المقترحة متعلقة بمجالات مثل: مواءمة القوانين، والانضمام إلى صكوك دولية أو محلية قائمة تعنى بالجريمة السيبرانية، ووضع صكوك دولية جديدة، وتعزيز آليات التعاون الدولي والحصول على الأدلة الواقعة خارج نطاق الولاية القضائية بشكل عملي، وبناء قدرات هيئات إنفاذ القانون ومؤسسات العدالة الجنائية.[1]

وقد أبرزت العديد من الدول أهمية إتاحة آلية سريعة لإجراءات التعاون الدولي في المسائل الجنائية التي تنطوي على جريمة سيبرانية. وفي هذ الصدد، اقترحت بعض الدول تعزيز شبكات أجهزة الشرطة القائمة غير الرسمية، بيد أن بعض الدول الأخرى افترضت تحقيق ذلك من خلال تطوير قنوات التعاون الدولية القائمة أكثر، بما في ذلك الاتفاقيات الثنائية ومتعددة الأطراف. كما أكدت بعض الدول أن كل الخيارات يجب أن تنفذ بما يتماشى مع المعايير الدولية لحقوق الإنسان، بما في ذلك الحق في حرية التعبير والخصوصية.

وقد أوصت بعض الدول بأن الانضمام إلى اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية من شأنه تعزيز التعاون الدولي واِتِّساق القوانين الوطنية المتعلقة بالجريمة السيبرانية، في حين أن بعض الدول الأخرى أوصت بأنه يمكن تعزيز مواءمة التشريعات من خلال وضع أحكام قانونية نموذجية على مستوى الأمم المتحدة.

كما أوصى عدد من الدول بأنه يتعين وضع معايير دولية بشأن تحقيقات إنفاذ القانون فيما يتعلق بالبيانات خارج الحدود الإقليمية، بهدف توضيح علاقة هذه التحقيقات مع مبادئ السيادة الوطنية.

واقترحت عدد من الدول تعزيز المساعدة الفنية لهيئات إنفاذ القانون، وأجهزة النيابة العامة والسلطات القضائية في مجال منع الجريمة السيبرانية ومكافحتها.

في ضوء المقترحات المقدمة من الدول الأعضاء والاستنتاجات الرئيسية، إرتأت الدراسة أن الخيارات المتاحة لتعزيز التدابير القانونية واقتراح تدابير قانونية أو تدابير أخرى جديدة وطنية ودولية للتصدي للجريمة السيبرانية، يمكن أن تشمل واحدا أو أكثر مما يلي:

(أ) صوغ أحكام نموذجية دولية بشأن تجريم الأفعال الأساسية التي تمثل جريمة سيبرانية، بغية دعم الدول في القضاء على الملاذات الآمنة من خلال اعتماد عناصر مشتركة للجريمة:

[1] الاستبيان الخاص بدراسة الجريمة السيبرانية، السؤال رقم 11.

(1) يمكن أن تُبقى الأحكام على نهج الصكوك القائمة فيما يتعلق بالجرائم التي تمس بسرية النظم والبيانات الحاسوبية وسلامتها وحقوق النفاذ إليها؛

(2) يمكن أن تشمل الأحكام أيضا الجرائم "التقليدية" المرتكبة أو الميسّرة باستخدام النظم الحاسوبية، على أن يقتصر ذلك على الحالات التي تُعتبر فيها نهج التجريم القائمة غير كافية؛

(3) يمكن أن تعالج الأحكام مجالات غير مشمولة في الصكوك القائمة، كتجريم البريد الإلكتروني الطفيلي (SPAM)؛

(4) يمكن وضع الأحكام على نحو ينسجم مع أحدث المعايير الدولية لحقوق الإنسان بشأن التجريم، بما في ذلك بصورة خاصة، الأحكام التعاهدية للحق في حرية التعبير.

(5) من شأن استخدام الدول للأحكام أن يقلل إلى أدنى حد التحديات التي تطرحها مشكلة ازدواجية التجريم في التعاون الدولي؛

(ب) صوغ أحكام نموذجية دولية بشأن صلاحيات التحقيق الخاصة بالأدلة الإلكترونية، بغية دعم الدول في ضمان وجود الأدوات الإجرائية الضرورية للتحقيق في الجرائم التي تشتمل على أدلة إلكترونية:

(1) يمكن أن ترتكز الأحكام على النهج المعتمد في الصكوك القائمة، بما في ذلك أوامر الحفظ العاجل للبيانات وأوامر الحصول على البيانات المخزّنة والآنية؛

(2) يمكن أن توفّر الأحكام إرشادات بشأن توسيع نطاق الصلاحيات التقليدية، مثل التحري بشأن الأدلّة السيبرانية ومصادرتها؛

(3) يمكن أن توفّر الأحكام إرشادات بشأن تطبيق الضمانات المناسبة فيما يخص تقنيات التحقيق التدخلية، مع مراعاة القانون الدولي لحقوق الإنسان، بما في ذلك الأحكام التعاهدية التي تحمي الحق في الخصوصية؛

(ج) صوغ أحكام نموذجية بشأن الولاية القضائية، من أجل توفير أسس فعّالة مشتركة للولاية القضائية في المسائل الجنائية الخاصة بالجريمة السيبرانية:

(1) يمكن أن تتضمن الأحكام أسسا كتلك المستمدة من مبدأ الإقليمية الموضوعية ومبدأ الآثار الجوهرية؛

(2) يمكن أن تتضمن الأحكام إرشادات لمعالجة المسائل المتعلقة بالولاية القضائية المشتركة؛

(د) صوغ أحكام نموذجية بشأن التعاون الدولي فيما يتعلق بالأدلّة الإلكترونية، بغية إدراجها في الصكوك الثنائية أو متعددة الأطراف، بما في ذلك إعداد معاهدة نموذجية منقّحة للأمم المتحدة بشأن المساعدة

القانونية المتبادلة، وفقا للاقتراحات الواردة في دليل المناقشة الخاص بالمؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية:

(1) يمكن أن تركّز الأحكام على آليات التعاون العملي التي يمكن إدراجها في الصكوك القائمة من أجل حفظ وتقديم الأدلّة الإلكترونية، في المسائل الجنائية، في الوقت المناسب؛

(2) يمكن أن تتضمن الأحكام مقتضيات لتحديد جهات اتصال سريعة الاستجابة فيما يخص الأدلّة الإلكتورنية وجداول زمنية متّفق عليها للاستجابات؛

(هـ) صوغ صك متعدد الأطراف بشأن التعاون الدولي فيما يتعلق بالأدلّة الإلكترونية في المسائل الجنائية، بغية توفير آلية دولية للتعاون جيد التوقيت بغية حفظ الأدلّة الإلكترونية والحصول عليها:

(1) يمكن أن يُضاف الصك باعتباره مكمّلا لمعاهدات التعاون الدولي القائمة، وأن يركّز بشكل أساسي على آلية لطلب الحفظ العاجل للبيانات لفترة زمنية محدَّدة؛

(2) يمكن أن يتضمن الصك أيضا أحكاما محدَّدة بشأن التعاون في تنفيذ تدابير تحقيق إضافية، بما في ذلك توفير البيانات المخزّنة وجمع آني للبيانات؛

(3) يَلزم تحديد نطاق تطبيق الصك، غير أنه يجب ألا يقتصر على "الجريمة السيبرانية" أو الجرائم "المتعلقة بالحاسوب"؛

(4) يمكن أن يقضي الصك بالاستجابة للطلبات في غضون فترة زمنية محدَّدة، وأن يحدِّد جهة اتصال واضحة لأغراض قنوات تنسيق الاتصالات، بالاستناد إلى الآليات القائمة العاملة على مدار الساعة، بدلا من إنشاء آليات جديدة تفضي إلى ازدواجية الجهود؛

(5) يمكن أن يتضمن الصك ضمانات تعاون دولي تقليدية، واستثناءات مناسبة فيما يتعلق بحقوق الإنسان؛

(و) صوغ صك شامل متعدد الأطراف بشأن الجريمة السيبرانية، يصنع معالم نهج دولي في مجالات التجريم، والصلاحيات الإجرائية، والولاية القضائية، والتعاون الدولي:

(1) يمكن أن يتضمن الصك عناصر من جميع الخيارات المشار إليها أعلاه في شكل ملزم ومتعدد الأطراف؛

(2) يمكن أن يستند الصك إلى القواسم المشتركة الأساسية القائمة في المجموعة الحالية للصكوك الدولية والإقليمية الملزمة وغير الملزمة؛

(ز) تعزيز الشراكات الدولية والإقليمية والوطنية، بما في ذلك الشراكات مع القطاع الخاص والمؤسسات الأكاديمية، من أجل توفير مساعدة تقنية معزّزة لمنع الجريمة السيبرانية ومكافحتها في البلدان النامية:

(1) يمكن توفير المساعدة الفنية بالاستناد إلى معايير توضع من خلال أحكام نموذجية على النحو المبيَّن في الخيارات المشار إليها أعلاه.

(2) يمكن توفير المساعدة الفنية من خلال التركيز على أصحاب مصالح متعددين، بما في ذلك من ممثلين من القطاع الخاص والمؤسسات الأكاديمية.

موجز تنفيذي

الموصولية والجريمة السيبرانية

كان عدد الموصولين بالإنترنت في عام 2011، لا يقل عن 2.3 بليون نسمة، أي ما يعادل أكثر من ثلث مجموع سكان العالم. ويعيش أكثر من 60 في المائة من جميع مستخدمي الإنترنت في البلدان النامية، ولا يتجاوز عمر 45 في المائة من مجموع مستخدمي الإنترنت الـ25 عاما. وبحلول عام 2017، من المتوقع أن تناهز نسبة المشتركين في خدمات الإنترنت النقالة ذات النطاق العريض 70 في المائة من المجموع الكلي لسكان العالم. وبحلول عام 2020، سيفوق عدد الأجهزة المتصلة بالشبكة (الأشياء "المتصلة بالإنترنت") عدد الناس بنسبة ستة إلى واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت. ففي عالم الغد المتسم بالموصولية البالغة، سيصعب تصوُّر وقوع "جريمة حاسوبية" وربما أيِّ جريمة أخرى لا تنطوي على أدلة إلكترونية تتعلق بالموصولية بواسطة بروتوكول الإنترنت (IP).

وتتوقف "تعاريف" الجريمة السيبرانية، في المقام الأول، على الغرض من استخدام المصطلح. فالجريمة السيبرانية الأساسية تتمثل في عدد محدود من الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها. أمَّا الأعمال المنفّذة بواسطة الحواسيب والرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار، بما في ذلك أشكال الجريمة المتصلة بالهوية وبمحتوى الحواسيب (والتي تندرج كلها ضمن نطاق أوسع من معنى مصطلح "الجريمة السيبرانية")، فلا يمكن تطويعها بسهولة لتنضوي ضمن تعاريف قانونية لمصطلح جامع. ويلزم تعريف الأعمال الأساسية التي تشكِّل جريمة سيبرانية، وإن كان "تعريف" الجريمة السيبرانية لا يتسم بنفس القدر من الأهمية فيما يخص الأغراض الأخرى، كتحديد نطاق صلاحيات الهيئات المختصة بالتحريات والتعاون الدولي، حيث يفضّل التركيز على الأدلة الإلكترونية فيما يخص أيِّ جريمة، بدلا من التركيز على تركيبة واسعة واصطناعية لـ "الجريمة السيبرانية".

الصورة العالمية

شهدت بلدان عديدة زيادة هائلة في الموصولية العالمية في وقت يتَّسم بتحولات اقتصادية وديمغرافية، وبتزايد التفاوت في الدخل، وتقييد الإنفاق في القطاع الخاص، وانخفاض السيولة المالية. وعلى الصعيد العالمي، لاحظ موظّفو إنفاذ القانون المشاركون في الدراسة ارتفاع مستويات الجريمة السيبرانية، حيث يستغل

الجريمة السيبرانية والإيقاع الإجرامي التقليدي بالضحايا

المصدر: تقديم مكتب الأمم المتحدة المعني بالمخدرات والجريمة لتقرير نورتن بشأن الجريمة السيبرانية واستطلاعات ضحايا الجريمة.

الأفراد والجماعات الإجرامية المنظمة الفرص الجديدة المتاحة لارتكاب الجرائم بغية تحقيق الأرباح والمكاسب الشخصية. وتشير التقديرات إلى أنَّ مصدر أكثر من 80 في المائة من الجريمة السيبرانية هو شكل من أشكال النشاط المنظم، حيث تقوم الأسواق السوداء للجرائم السيبرانية على دورة تتسم بإعداد البرمجيات الخبيثة والفيروسات الحاسوبية والتحكُّم بشبكات حاسوبية ("اعتداءات البوت نت – Botnet") وتلقُّف البيانات الشخصية والمالية وبيع البيانات والمتاجرة بالمعلومات المالية. ولم يعد مرتكبو الجريمة السيبرانية بحاجة إلى مهارات أو تقنيات معقّدة. ففي سياق البلدان النامية بصورة خاصة، ظهرت ثقافات فرعية تضم شبانا يرتكبون أعمال احتيال مالي بالحواسيب، بدأ كثيرون منهم بالتورط في الجريمة السيبرانية في أواخر سنوات المراهقة.

وعلى الصعيد العالمي، تشمل الجريمة السيبرانية طائفة واسعة من الجرائم المرتكبة بدافع مالي، والجرائم المتصلة بالمحتوى الحاسوبي، فضلا عن الأعمال التي تمس بسرية النظم الحاسوبية، وسلامتها وقابلية النفاذ إليها. غير أنَّ تصوّرات الخطر والتهديد النسبيَّين تختلف بين الحكومات ومؤسسات القطاع الخاص. وفي الوقت الراهن، لا تمثّل إحصاءات الجرائم المسجّلة لدى الشرطة أساسا سليما للمقارنات الدولية، على الرغم من أنَّ هذه الإحصاءات غالبا ما تكون مهمة لوضع السياسات على الصعيد الوطني. ويرى ثلثا البلدان أنَّ نظم إحصاءات الشرطة لديها غير كافية لتسجيل الجريمة السيبرانية. وترتبط معدّلات الجريمة السيبرانية المسجّلة لدى الشرطة بمستويات التنمية القُطرية وقدرة الشرطة المتخصصة، أكثر من ارتباطها بمعدّلات الجرائم المرتكبة.

وتمثّل استبيانات الإيذاء الإجرامي أساسا أسلم للمقارنة. وتُظهر هذه الاستبيانات أنَّ حالات التأذي الفردية من الجريمة السيبرانية هي أكثر بكثير من حالات التأذي من أشكال الجرائم "التقليدية". وتتراوح معدّلات التأذي، من تزوير بطاقات الائتمان وانتحال الشخصية على الإنترنت والوقوع ضحية لمحاولات تصيُّد احتيالي ومحاولات اطلاع دون إذن على حسابات البريد الإلكتروني، بين 1 و17 في المائة من نسبة السكان الذين يستخدمون الإنترنت في 21 بلدا في جميع أنحاء العالم، مقارنة بمعدلات التأذّي من السطو والسلب وسرقة السيارات التقليدية التي تقل عن 5 في المائة من نسبة السكان في هذه البلدان نفسها. وكانت معدلات الإيذاء بسبب الجريمة السيبرانية أعلى في البلدان التي تشهد مستويات نمو منخفضة، مما يُبرز الحاجة إلى تعزيز جهود منع الجرائم في هذه البلدان.

وأبلغت مؤسسات القطاع الخاص في أوروبا عن معدلات تأذي مماثلة – تراوحت بين 2 و16 في المائة – وكانت تتعلق بانتهاك البيانات بسبب الاقتحام أو التصيّد الاحتيالي. والساحة التي تُستخدَم فيها هذه الأدوات المختارة لارتكاب الجرائم، مثل "اعتداءات البوت نت"، هي ساحة عالمية. فقد كان أكثر من مليون عنوان فريد من عناوين بروتوكول الإنترنت يعمل على الصعيد العالمي كخادم "بوت نت" للتحكُّم في شبكات الحواسيب ومراقبتها في عام 2011. ومثّل محتوى الإنترنت أيضا مصدر قلق كبير للحكومات، فمن المواد المراد حذفها منه المواد الإباحية المتعلقة بالأطفال، والخطابات المفعمة بالكراهية، ومواد التشهير، وانتقاد الحكومات، الأمر الذي أثار شواغل متعلقة بقانون حقوق الإنسان في بعض الحالات. ويُقدَّر أنَّ حوالي 24 في المائة من

إجمالي حركة الإنترنت العالمية تنتهك حقوق النشر، إذ تشمل تنزيل كثير من المواد من مواقع تبادل الملفات بين النظراء من مستخدمي الإنترنت (P2P)، ولاسيّما في بلدان في أفريقيا وأمريكا الجنوبية وغرب آسيا وجنوبها.

التشريعات والأطر

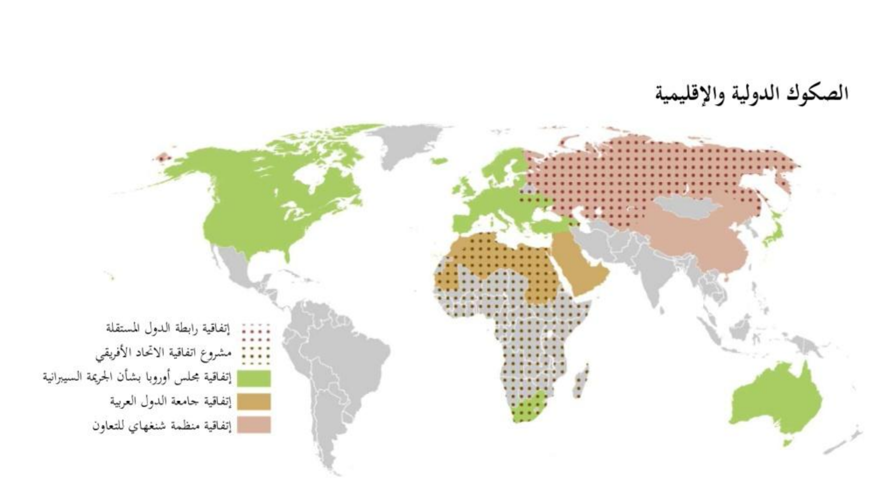
تؤدي التدابير القانونية دورا رئيسيا في منع الجريمة السيبرانية ومكافحتها. وهذه التدابير ضرورية في جميع المجالات، بما في ذلك التجريم، والصلاحيات الإجرائية، والولاية القضائية، والتعاون الدولي، ومسؤولية مقدّمي خدمات الإنترنت. وعلى الصعيد الوطني، كثيرا ما تتعلق قوانين الجريمة السيبرانية، القائمة والجديدة (أو المخطط لها) على حدٍّ سواء، بالتجريم، مما يدل على التركيز بصفة رئيسية على تجريم أفعال متخصّصة تغطي الجريمة السيبرانية الأساسية. غير أنَّ البلدان تُسلِّم أكثر فأكثر بالحاجة إلى تشريعات في مجالات أخرى. ومقارنة بالقوانين القائمة، تعالج القوانين الجديدة أو المخطط لها الخاصة بالجريمة السيبرانية إجراءات التحقيق والولاية القضائية والأدلّة الإلكترونية والتعاون الدولي. وعلى الصعيد العالمي، رأى أقل من نصف البلدان المجيبة عن الاستبيان أنَّ أطر القوانين الجنائية والإجرائية الخاصة بها كافية، وإن كانت تنطوي على تباينات إقليمية كبيرة. ففي حين أبلغ أكثر من ثلثي البلدان في أوروبا عن وجود تشريعات كافية، كانت الصورة معكوسة في أفريقيا والأمريكيتان وآسيا وأوقيانوسيا، حيث رأى أكثر من ثلثي البلدان أنَّ قوانينها كافية جزئيا فقط، أو غير كافية البتة. وأشار نصف البلدان التي أبلغت أنَّ قوانينها غير كافية أيضا إلى قوانين جديدة أو مخطط لها، مما يسلّط الضوء على الحاجة الملحَّة إلى تعزيز التشريعات في هذه المناطق.

وشهد العقد الأخير تطورات مهمة على صعيد إصدار الصكوك الدولية والإقليمية الملزمة وغير الملزمة الرامية إلى التصدّي للجريمة السيبرانية. ويمكن تحديد خمس مجموعات من الصكوك، أُعدَّت في إطار هيئات أو استُقيت من هيئات هي: (1) مجلس أوروبا أو الاتحاد الأوروبي، و(2) كومنولث الدول المستقلة أو منظمة شنغهاي للتعاون، و(3) المنظمات الأفريقية الحكومية الدولية، و(4) جامعة الدول العربية، و(5) الأمم المتحدة. ويثري كل من هذه الصكوك، الصكوك الأخرى إثراء كبيرا، في مجالات منها على وجه الخصوص المفاهيم والنهج التي وُضعت في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية. ويظهر تحليل مواد 19 صكا متعدد الأطراف متصلا بالجريمة السيبرانية وجود أحكام أساسية مشتركة من جهة، وتباينا كبيرا في المجالات الموضوعية المتناولة من جهة أخرى.

وعلى الصعيد العالمي، وقَّع أو صدَّق 82 بلدا على صك ملزم بشأن الجريمة السيبرانية.[1] وبالإضافة إلى العضوية الرسمية والتنفيذ، فإن هذه الصكوك متعددة الأطراف المتعلقة بالجريمة السيبرانية أثرت بشكل غير مباشر على القوانين الوطنية، من خلال استخدامها كنموذج من جانب الدول غير الأطراف فيها، أو من خلال تأثير تشريعات الدول الأطراف فيها على البلدان الأخرى. وتتناسب العضوية في الصكوك متعددة الأطراف المتعلقة بالجريمة

[1] صك واحد أو أكثر من الصكوك التالية: اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، أو اتفاقية جامعة الدول العربية لمكافحة جرائم تقنية المعلومات، أو اتفاقية دول الكومنولث المستقلة حول التعاون في مكافحة الجرائم في مجال المعلومات الحاسوبية، أو اتفاق منظمة شنغهاي للتعاون في ميدان أمن المعلومات على الصعيد الدولي.

السيبرانية مع الزيادة المتصوّرة في مدى كفاية القانون الجنائي والإجرائي الوطني، مما يدل على أنَّ الأحكام الحالية متعددة الأطراف في هذه المجالات تُعتبر فعّالة عموما. وفيما يخص البلدان التي يفوق عددها الأربعين والتي قدّمت المعلومات، كانت اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية هي الصك المتعدد الأطراف الذي استندت إليه بصفة رئيسية لوضع التشريعات الخاصة بالجريمة السيبرانية. وإجمالا، استخدم حوالي نصف هذه البلدان صكوكا متعددة الأطراف مندرجة في "المجموعات" الأخرى.



وأفاد ثلث البلدان المجيبة عن الاستبيان عموما بأنَّ تشريعاتها تتناسق إلى حد كبير، أو إلى حد كبير جدا، مع تشريعات البلدان التي تُعتبر علاقاتها بها مهمة لأغراض التعاون الدولي. غير أنَّ الوضع يتباين على الصعيد الإقليمي، إذ ترتفع مستويات التنسيق المبلّغ عنها في الأمريكتين وأوروبا. وقد يكون ذلك نتيجة لاستخدام بعض المناطق لصكوك متعددة الأطراف مصممة بطبيعتها لأداء دور في تنسيق التشريعات. وقد يعزى عدم الاتساق على المستوى الدولي وتنوّع القوانين الوطنية، من حيث تجريم الأعمال التي تعتبر جرائم إلكترونية والقواعد التي تحدّد الولاية القضائية وآليات التعاون، إلى وجود صكوك متعددة بشأن الجريمة السيبرانية لها نطاق موضوعي وجغرافي مختلف. والحال أنَّ التباين يعتري الصكوك والمناطق بسبب الاختلافات القانونية والدستورية فيها، بما في ذلك ما يسود فيها من مفاهيم مختلفة بشأن الحقوق والخصوصية.

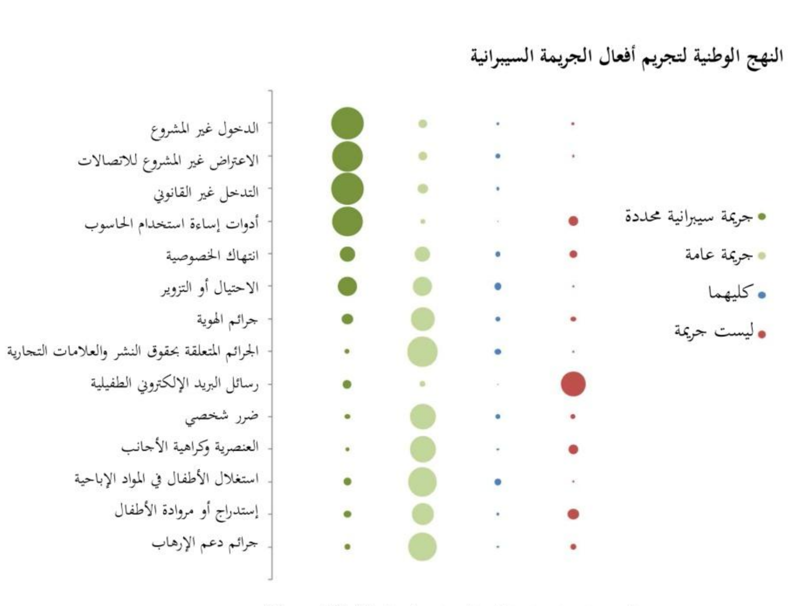
التجريم

جمعت المعلومات بشأن القوانين الجنائية المتعلقة بالجريمة السيبرانية من خلال الاستبيان الخاص بالدراسة، ومن خلال تحليل المصادر الرئيسية للتشريعات المتوافرة التي جمعتها الأمانة.[1] وأشار الاستبيان إلى 14 فعلا يندرج عادة ضمن مفاهيم الجريمة السيبرانية.[2] وتبيَّن من إجابات البلدان على الاستبيان أنَّ هذه الأفعال الـ14 مجرَّمة على نطاق واسع، باستثناء الجرائم المتعلقة برسائل البريد الإلكتروني الطفيلي (SPAM) بصفة رئيسية،

[1] لقد حُلّل المصدر الرئيسي لتشريعات 97 دولة عضوا، بما في ذلك 56 دولة أجابت عن الاستبيان، وكان توزيعها الإقليمي على النحو التالي: أفريقيا (15) والأمريكيتان (22) وآسيا (24) وأوروبا (30) وأوقيانوسيا (6).

[2] النفاذ غير المشروع إلى نظام حاسوبي؛ والنفاذ غير المشروع إلى بيانات الحواسيب أو اعتراض هذه البيانات أو الحصول عليها؛ والتدخل غير المشروع في البيانات أو النظم؛ وإنتاج أو توزيع أو حيازة أدوات لإساءة استعمال الحواسيب؛ وانتهاك الخصوصية أو تدابير حماية بيانات؛ والاحتيال أو التزوير بواسطة الحواسيب؛ وجرائم الهوية المرتكبة بواسطة الحواسيب؛ وجرائم حقوق النشر والعلامات التجارية المرتكبة بواسطة الحواسيب؛ والأعمال المرتكبة بواسطة الحواسيب والتي تتسبب بضرر شخصي؛ والأعمال المرتكبة بواسطة الحواسيب والتي تنطوي على عنصرية أو كراهية للأجانب؛ وإنتاج أو توزيع أو حيازة المواد الإباحية المتعلقة بالأطفال بواسطة الحواسيب؛ وإغواء أو "مراودة" الأطفال بواسطة الحواسيب؛ وأعمال دعم الجرائم الإرهابية بواسطة الحواسيب.

وكذلك إلى حد ما الجرائم المتعلقة بأدوات إساءة استعمال الحواسيب والعنصرية وكراهية الأجانب وإغواء أو "مراودة" الأطفال على الإنترنت. ويجسّد هذا الأمر نوعا من توافق الآراء الأساسي على ما يُعاقب عليه من السلوكيات الإجرامية السيبرانية. وأبلغت بلدان عن بعض الجرائم الإضافية غير المذكورة في الاستبيان، والمتعلقة بصفة رئيسية بمحتوى الحواسيب، بما في ذلك تجريم المواد الفاحشة، ولعب القمار على الإنترنت، والأسواق غير المشروعة على الإنترنت من قبيل أسواق الاتجار بالمخدرات والبشر. وفيما يخص الأفعال الـ14 المذكورة، أبلغت بلدان بأنها تستند إلى الجرائم الخاصة بالفضاء الإلكتروني لتحديد الجرائم السيبرانية الأساسية التي تمس بسرية النظم الحاسوبية وسلامتها وقواعد النفاذ إليها. وفيما يخص الأشكال الأخرى من الجريمة السيبرانية، استخدمت الجرائم العامة (غير السيبرانية) في أغلب الأحيان. غير أنه أُبلغ عن الأخذ بالنهجين فيما يخص الأفعال المرتكبة بواسطة الحواسيب والتي تشتمل على خرق السرية أو الاحتيال أو التزوير أو ارتكاب جرائم متصلة بالهوية.



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 25-38. (ع=61)

ولئن كان هناك توافق رفيع المستوى في الآراء بشأن مجالات التجريم الواسعة، فإنَّ التحليل المفصّل للأحكام الواردة في التشريعات المرجعية يكشف عن نُهُج متباينة. ذلك أنَّ الجرائم التي تنطوي على *نفاذ* غير مشروع إلى النظم الحاسوبية والبيانات تختلف باختلاف موضوع الجريمة (بيانات، أو نظم، أو معلومات) ومستوى التجريم، أي تجريم النفاذ "بحد ذاته" أو اقتضاء وجود نية أخرى من وراء النفاذ مثل التسبُّب في خسائر أو أضرار. وتختلف النية المطلوب وجودها ليكون الفعل المرتكب جريمة باختلاف نهج تجريم *التدخُّل* في النظم الحاسوبية أو البيانات الحاسوبية. فمعظم البلدان تقضي بأن يكون التدخُّل في النظم أو البيانات متعمدا ليعتبر جريمة، في حين تجرِّم بلدان أخرى التدخُّل المستهتر فيها. وفيما يتعلق بالتدخُّل في البيانات الحاسوبية، يتراوح السلوك الذي يشكّل تدخلا فيها بين إتلافها أو حذفها وصولا إلى تغييرها أو قمعها أو إدخالها أو نقلها. ويختلف تجريم التدخُّل غير المشروع تبعا لما إذا كان الجرم محصورا بنقل البيانات غير العمومية، وما إذا كان محصورا بالتدخُّل "بواسطة الوسائل التقنية". ولا تجرِّم جميع البلدان *أدوات إساءة استعمال الحواسيب*. أمَّا في البلدان التي تجرِّمها، فتبرز الاختلافات تبعا لما إذا كان الجرم يشمل حيازة أو توزيع أو استعمال البرمجيات (كالبرمجيات الخبيثة) و/أو رموز النفاذ إلى الحواسيب (ككلمات مرور الضحية). ومن منظور التعاون الدولي، قد يكون لهذه الاختلافات تأثير على الاستنتاجات المتعلقة بازدواجية التجريم بين البلدان.

واعتمدت بلدان عديدة مصطلح جرائم الفضاء الإلكتروني فيما يتعلق بجرائم الاحتيال والتزوير والجرائم المتصلة بالهوية المرتكبة بواسطة الحاسوب، في حين قامت بلدان أخرى بتوسيع نطاق الأحكام العامة المتعلقة بالاحتيال أو السرقة، أو اعتمدت على الجرائم التي تشمل العناصر المكونة ذات الصلة — كالنفاذ غير المشروع والتدخُّل في البيانات والتزوير، في حالة الجرائم المتعلقة بالهوية. وقد جُرِّم على نطاق واسع عدد من الجرائم المتصلة بالمحتوى، لا سيّما الجرائم المنطوية على مواد إباحية متعلقة بالأطفال. غير أنَّ الاختلافات تبرز بشأن تعريف مصطلح "الطفل"، والقيود المتعلقة بالمواد "البصرية" أو استبعاد المواد المحاكية، والأفعال المشمولة. وعلى الرغم من أنَّ الغالبية العظمى من البلدان تجرِّم، على سبيل المثال، إنتاج وتوزيع المواد الإباحية المتعلقة بالأطفال، يظهر تباين أكبر في تجريم حيازة هذه المواد والاطلاع عليها. وفيما يتعلق بانتهاك حقوق النشر والعلامات التجارية بواسطة الحواسيب، أبلغ أكثر البلدان عن تطبيق الجرائم الجنائية العامة على الأفعال المرتكبة عمدا وعلى نطاق تجاري.

ودفع الاستخدام المتزايد لوسائل التواصل الاجتماعي ومحتوى الإنترنت الذي ينتجه المستخدمون أنفسهم، الحكوماتِ إلى اتخاذ تدابير تنظيمية، من بينها اللجوء إلى القانون الجنائي، والدعوة إلى احترام الحق في حرية التعبير. وأبلغت البلدان المجيبة عن الاستبيان عن قيود مختلفة على التعبير، ومن ذلك القيود المفروضة على التشهير والإهانة والتهديد والتحريض على الكراهية وإهانة المشاعر الدينية والمواد الفاحشة وتقويض الدولة. ويُجسَّد العنصر الاجتماعي والثقافي لبعض القيود ليس فقط في القانون الوطني وإنما أيضا في الصكوك متعددة الأطراف. فبعض الصكوك الإقليمية المتعلقة بالجريمة السيبرانية تشمل على سبيل المثال جرائم واسعة النطاق بشأن انتهاك الآداب العامة والمواد الإباحية والمبادئ أو القيم الدينية أو العائلية.

ويعمل القانون الدولي لحقوق الإنسان بمثابة سيف ودرع على حد سواء، إذ إنه يقضي بتجريم أشكال تعبير متطرفة (محدودة)، ويحمي أشكال تعبير أخرى. ومن ثم يتعيّن على الدول الأطراف في الصكوك الدولية لحقوق الإنسان فرض بعض القيود على حرية التعبير، بما في ذلك التحريض على الإبادة الجماعية والكراهية التي تشكّل تحريضا على التمييز أو العداء أو العنف وتحريضا على الإرهاب ودعاية للحرب. ومن جهة أخرى، ثمة "هامش تقدير" يتيح للبلدان المجال لوضع حدود للتعبير المقبول بما يتماشى مع ثقافاتها وتقاليدها القانونية. ومع ذلك، يكون للقانون الدولي لحقوق الإنسان دور عند نقطة معينة. فتطبيق القوانين الجنائية المتعلقة بالتشهير وعدم احترام السلطة والإهانة مثلا، على التعبير على الإنترنت، سيواجه صعوبات كبيرة لإثبات تناسب التدابير وملاءمتها واتِّسامها بأقل قدر من التدخُّل. وعندما يكون المحتوى غير قانوني في بلد ما، ويكون إنتاجه ونشره قانونيا في بلد آخر، سيتعين على الدول التركيز في تدابير العدالة الجنائية التي ستتخذها على الأشخاص الذين يطّلعون على المحتوى الذي يعدّ غير قانوني ضمن ولايتها القضائية الوطنية، بدلا من التركيز على المحتوى المنتج خارج البلد.

سلطات إنفاذ القانون والتحقيقات

أشار أكثر من 90 في المائة من البلدان المجيبة عن الاستبيان إلى أنَّ السلطات المسؤولة عن إنفاذ القانون تبلَّغ بمعظم الجرائم السيبرانية من خلال التقارير المقدّمة من الضحايا الأفراد أو الضحايا من الشركات. وقدَّرت البلدان المجيبة عن الاستبيان أنَّ نسبة التأذّي الفعلي من الجريمة السيبرانية المبلّغ عنها إلى الشرطة تبدأ من واحد في المائة. وتشير دراسة استقصائية عالمية للقطاع الخاص إلى أنَّ 80 في المائة من الضحايا الأفراد للجرائم السيبرانية الأساسية لا يبلغون الشرطة عن الجريمة. ويعزى تدني الإبلاغ عن هذه الجرائم إلى عدم الوعي بالإيذاء وآليات الإبلاغ، وإلى شعور الضحايا بالخجل والارتباك، وإلى تخوُّف الشركات من مخاطر متصورة على سمعتها. وأشارت السلطات في جميع مناطق العالم إلى المبادرات الرامية إلى تعزيز الإبلاغ عن تلك الجرائم، بما في ذلك عن طريق نظم الإبلاغ بالاتصال الحاسوبي المباشر وبالخطوط الهاتفية المباشرة وحملات التوعية العامة والتواصل مع القطاع الخاص وتعزيز توعية الشرطة وتبادل المعلومات. غير أنَّ تدابير التصدِّي للجريمة السيبرانية التي تتخذ لمعالجة حوادث معينة يجب أن تقترن بتحقيقات تكتيكية على المديين المتوسط والبعيد، تركز على أسواق الجريمة ومدبري المخططات الإجرامية. وتشارك سلطات إنفاذ القانون في البلدان المتقدمة في هذا المجال، بما في ذلك من خلال الوحدات السرية التي تستهدف المجرمين على مواقع الشبكات الاجتماعية وغرف الدردشة والرسائل الفورية ومواقع تبادل الملفات بين النظراء (P2P). وتنشأ التحديات التي ينطوي عليها التحقيق في الجريمة السيبرانية عن الابتكارات الإجرامية والصعوبات في الحصول على الأدلة السيبرانية والقيود على الموارد الداخلية والقدرات والقيود اللوجستية. وغالبا ما يلجأ المشتبه بهم إلى تقنيات إخفاء الهوية والتشويش، وتصل التقنيات الجديدة بسرعة إلى جمهور المجرمين الواسع من خلال أسواق الجريمة على الإنترنت.

النهج الوطنية لإجراءات التحري عن الجريمة السيبرانية

المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 42-51. (ع=55)

وتتطلب التحقيقات التي تجريها سلطات إنفاذ القانون في الجريمة السيبرانية مزيجا من تقنيات عمل الشرطة التقليدية والجديدة. فلئن أمكن تنفيذ بعض إجراءات التحقيق بواسطة التقنيات التقليدية، فإنه يصعب تكييف العديد من الإجراءات التي تستند إلى نهج قائم على مكان الأشياء لجعلها تستند إلى نهج قائم على تخزين البيانات السيبرانية وتدفق البيانات في الوقت الحقيقي. وأشار الاستبيان إلى عشرة إجراءات للتحقيق في الجريمة السيبرانية، بدءا من البحث العام والمصادرة

ووصولا إلى الإجراءات المتخصصة، كحفظ البيانات الحاسوبية.[1] وفي حين أبلغت البلدان في أكثر الأحيان عن وجود صلاحيات عامة (غير خاصة بالمجال الإلكتروني) في كل مستويات التحريات. وأبلغ عدد من البلدان أيضا عن تشريعات خاصة بالمجال الإلكتروني، ولاسيما لضمان التعجيل في حفظ البيانات الحاسوبية والحصول على بيانات المشتركين المخزّنة. وأبلغت بلدان عديدة عن عدم وجود صلاحيات قانونية لاتخاذ إجراءات متقدّمة، مثل التحاليل الجنائية الحاسوبية عن بُعد. وفي حين أنه يمكن توسيع نطاق الصلاحيات الإجرائية التقليدية لتشمل المجال الإلكتروني، فقد يؤدي هذا النهج في العديد من الحالات إلى أوجه عدم يقين قانوني وتحديات بشأن مشروعية جمع الأدلة، وبالتالي مقبوليتها. وعموما، ثمة قواسم مشتركة أساسية في النُهج الوطنية لصلاحيات التحقيق في الجريمة السيبرانية، أقل من القواسم المشتركة الأساسية في تجريم العديد من أفعال الجريمة السيبرانية.

وبصرف النظر عن الشكل القانوني لصلاحيات التحقيق، تستخدم جميع السلطات المجيبة عن الاستبيان البحث والمصادرة للاستحواذ الفعلي على المعدات الحاسوبية والحصول على البيانات الحاسوبية. وتستخدم غالبية البلدان أيضا أوامر قضائية للحصول على البيانات الحاسوبية المخزنة من مقدّمي خدمات الإنترنت. وخارج أوروبا، أبلغ حوالي ثلث البلدان عن تحديات في إقناع أطراف ثالثة لها علاقة بالتحقيق بتقديم المعلومات. ويستخدم حوالي ثلاثة أرباع البلدان إجراءات تحقيق متخصصة، كجمع البيانات في الوقت الحقيقي أو التعجيل في حفظها. ويتطلب استخدام إجراءات التحقيق عادة حدّا أدنى من الأدلة الأولية أو تقريرا عن وقوع جريمة إلكترونية. أمّا الإجراءات الأكثر تدخلا، كتلك التي تشتمل على جمع البيانات في الوقت الحقيقي أو النفاذ إلى محتوى البيانات، فتستلزم معايير أكثر صرامة، كوجود دليل على ارتكاب جريمة خطيرة أو دليل على وجود سبب محتمل أو أسس معقولة.

ويُعدّ التفاعل بين سلطات إنفاذ القانون ومقدّمي خدمات الإنترنت معقّدا بصفة خاصة. ولدى مقدّمي الخدمات المعلومات الخاصة بالمشتركين والفواتير وبعض سجلات الاتصال ومعلومات عن المواقع (كبيانات أبراج الاتصالات اللاسلكية الخاصة بمقدّمي خدمات الهواتف النقالة) ومحتوى الاتصالات، وقد تمثّل كل هذه العناصر أدلّة إلكترونية مهمة عن جريمة معيّنة. وتختلف المقتضيات القانونية الوطنية والسياسات المتّبعة في القطاع الخاص بشأن الاحتفاظ بالبيانات وإفشائها اختلافا كبيرا حسب البلد والقطاع ونوع البيانات. وقد أبلغت البلدان في معظم الأحيان عن اللجوء إلى أوامر قضائية للحصول على أدلة من مقدّمي الخدمات. ولكن سلطات إنفاذ القانون قد تتمكّن في بعض الحالات من الحصول بصورة مباشرة على بيانات المشتركين المخزّنة وبيانات حركة الاتصالات وحتى بيانات المحتوى. وفي هذا الصدد، أبلغ كثير من مؤسسات القطاع الخاص عن أخذها بسياسة أولية تقتضي مراعاة الأصول القانونية للإفشاء عن البيانات، وكذلك بنهج طوعي يتمثل في

[1] البحث عن المعدات أو البيانات الحاسوبية؛ ومصادرة المعدات أو البيانات الحاسوبية؛ والأمر بالحصول على معلومات المشتركين؛ والأمر بالحصول على بيانات حركة الاتصالات المخزّنة؛ والأمر بالحصول على بيانات المحتوى المخزّنة؛ وجمع بيانات حركة الاتصالات الآنية؛ وجمع بيانات المحتوى آنيا؛ والتعجيل في حفظ البيانات الحاسوبية؛ واستخدام أدوات التحاليل الجنائية الحاسوبية عن بُعد؛ والنفاذ عبر الحدود إلى نظم أو بيانات حاسوبية.

الاستجابة في بعض الظروف للطلبات المباشرة التي تقدمها سلطات إنفاذ القانون. وتساعد العلاقات غير الرسمية بين سلطات إنفاذ القانون ومقدّمي الخدمات، والتي أُبلغ عن وجودها في أكثر من نصف مجموع البلدان المجيبة عن الاستبيان، في عملية تبادل المعلومات وبناء الثقة. وأشارت الردود إلى أنَّ هناك حاجة إلى تحقيق التوازن بين الخصوصية ومراعاة الأصول القانونية من جهة، وبين إفشاء الأدلة في الوقت المناسب من جهة أخرى لضمان عدم تحوُّل القطاع الخاص إلى "معرقل" للتحقيقات.

وتنطوي تحقيقات الجريمة السيبرانية دائما على اعتبارات تتعلق بالخصوصية بموجب القانون الدولي لحقوق الإنسان. وتنصّ معايير حقوق الإنسان على أنَّ القوانين يجب أن تكون واضحة بما فيه الكفاية لتعطي دلالة كافية عن الظروف التي تخوِّل للسلطات استخدام إجراءات التحقيق، وأنَّه يجب أن تكون هناك ضمانات وافية وفعالة لمكافحة إساءة استخدام تلك الإجراءات. وأفادت بلدان بأنَّ قوانينها الوطنية تحمي حقوق الخصوصية، كما أبلغت عن مجموعة من القيود والضمانات في إطار التحقيقات. ولكن عندما تكون التحقيقات غير وطنية، يستتبع تباين مستويات حماية الخصوصية عدم القدرة على التنبؤ بقدرات سلطات إنفاذ القانون الأجنبية على الحصول على البيانات، وبالثغرات التي قد تنطوي عليها نظم حماية الخصوصية في الولاية القضائية المعنية.

وقد بدأ أكثر من 90 في المائة من البلدان التي أجابت عن الاستبيان بإنشاء هياكل متخصصة للتحقيق في الجريمة السيبرانية والجرائم التي تنطوي على أدلّة إلكترونية. لكن هذه الهياكل تفتقر في البلدان النامية إلى ما يكفي من الموارد والقدرات. ولدى البلدان الأقل نموّا عدد أقل بكثير من أفراد الشرطة المتخصصين، بمعدل يبلغ نحو 0.2 لكل 100,000 مستخدم إنترنت ضمن البلد المعني، في حين يكون هذا المعدّل أعلى بمرتين إلى خمس مرات في البلدان التي تفوقها تقدما. وأُفيد بأنَّ سبعين في المائة من الموظفين المتخصصين المكلفين بإنفاذ القوانين في البلدان الأقل نموا يفتقرون إلى المهارات والمعدات الحاسوبية، ولا يتلقى إلا نصفهم تدريبا أكثر من مرة واحدة في السنة. وأفاد أكثر من نصف البلدان المجيبة عن الاستبيان في أفريقيا وثلث البلدان في الأمريكتين بأنَّ الموارد المتاحة لسلطات إنفاذ القانون للتحقيق في الجريمة السيبرانية غير كافية. وعلى الصعيد العالمي، يرجّح أن تكون الصورة أسوأ. فلم يرد على الاستبيان على سبيل المثال إلا 20 في المائة من البلدان الخمسين الأقل نموّا في العالم. وأفادت جميع البلدان المجيبة عن الاستبيان في أفريقيا وأكثر من 80 في المائة من البلدان المجيبة في الأمريكتين وآسيا وأوقيانوسيا بأنها بحاجة إلى مساعدة تقنية. وكان المجال الذي كثر ذكره باعتباره يستلزم مساعدة تقنية هو أساليب التحرّي العامة المتعلقة بالجريمة السيبرانية. وقد أشار 60 في المائة من البلدان التي تحتاج إلى المساعدة إلى أنَّ وكالات إنفاذ القانون فيها بحاجة إلى هذا النوع من المساعدة.

الأدلة الإلكترونية والعدالة الجنائية

إنَّ الأدلة هي السبيل إلى تحديد الوقائع ذات الصلة بذنب أو براءة الفرد الجارية محاكمته. والأدلة الإلكترونية هي كل المواد الإثباتية التي توجد بشكل إلكتروني أو رقمي، والتي يمكن تخزينها أو نقلها. وقد تتخذ

شكل ملفات حاسوبية أو مواد منقولة أو سجلات أو بيانات فوقية أو بيانات شبكية. وتهتم التحاليل الجنائية الرقمية باستعادة المعلومات — التي كثيرا ما تتسم بسرعة زوالها وسهولة المساس بها – والتي قد تكون قيّمة لأغراض الأدلة. وتتضمن تقنيات التحاليل الجنائية إنشاء نسخ "مطابقة تماما" من المعلومات المخزنة والمحذوفة، واستخدام برامج "منع الكتابة" من أجل ضمان عدم تحريف المعلومات الأصلية، واستخدام خوارزميات "تجزئة" للملفات المشفّرة، أو استخدام التوقيعات الرقمية، بغية إظهار أي تعديلات تدخل على المعلومات. وأفاد معظم البلدان تقريبا بأنَّ لديها بعض القدرات في مجال التحاليل الجنائية الرقمية. غير أنَّ العديد من البلدان المجيبة عن الاستبيان، من جميع المناطق، أشار إلى عدم كفاية عدد المحققين المختصين في التحاليل الجنائية وإلى تباين القدرات على الصعيد الفيدرالي وصعيد الدولة، وإلى الافتقار إلى أدوات التحليل الجنائي، وتراكم الأعمال غير المنجزة بسبب الكميات الهائلة من البيانات اللازم تحليلها. وأفاد نصف البلدان بأنَّ المشتبه بهم يلجؤون إلى التشفير، مما يجعل الحصول على هذا النوع من الأدلة بدون رمز التشفير صعبا ويستغرق وقتا طويلا. وفي معظم البلدان، تقع مهمة تحليل الأدلة السيبرانية على عاتق سلطات إنفاذ القانون. غير أنه يتعيّن على المدّعين العامين معاينة وفهم الأدلة السيبرانية من أجل إقامة الحجة عند المحاكمة. وقد أفادت جميع البلدان في أفريقيا وثلث البلدان في مناطق أخرى بعدم كفاية الموارد المتاحة للمدّعين العامين للقيام بذلك. وتكون لدى المدّعين العامين مهارات حاسوبية أقل مستوى عادة من المهارات الحاسوبية للمحققين. وعلى الصعيد العالمي، أفاد نحو 65 في المائة من البلدان المجيبة عن الاستبيان بوجود نوع من التخصص في الجريمة السيبرانية لدى المدّعين العامين. ولم يبلغ سوى 10 في المائة من البلدان عن وجود دوائر قضائية متخصصة. ويتولّى النظر في الأغلبية العظمى من قضايا الجريمة السيبرانية قضاة غير متخصصين لا يتلقون في 40 في المائة من البلدان المجيبة عن الاستبيان أي نوع من التدريب المتصل بالجريمة السيبرانية. ويمثل تدريب القضاة في مجال قانون الجريمة السيبرانية وجمع الأدلة واكتساب المهارات الحاسوبية الأساسية والمتقدمة أولوية خاصة.

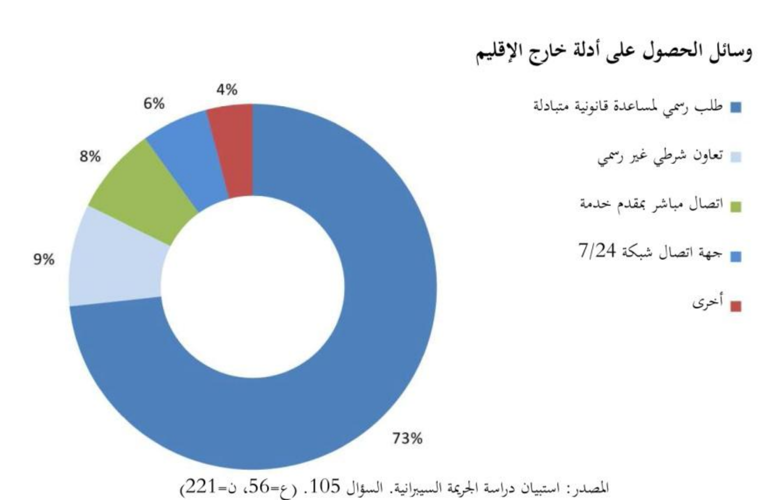
ولا يميّز أكثر من 60 في المائة من البلدان المجيبة عن الاستبيان تمييزا قانونيّا بين الأدلة الإلكترونية والأدلة المادية. ولئن كانت النُهج المتبعة مختلفة، فإنَّ بلدانا عديدة تعتبر هذه الممارسة جيدة، لأنها تضمن مقبولية الأدلة الإلكترونية على قدم المساواة مع جميع الأنواع الأخرى من الأدلة. ولا يعترف عدد من البلدان خارج أوروبا بالأدلة الإلكترونية على الإطلاق، مما يجعل الملاحقة القضائية لمرتكبي الجريمة السيبرانية وسائر الجرائم المثبتة بواسطة المعلومات الإلكترونية غير مجدية. وليس لدى بعض البلدان عموما قواعد إثبات منفصلة خاصة بالأدلة الإلكترونية، لكن عددا من البلدان أشار إلى مبادئ منها القواعد المتعلقة بأفضل دليل وبمدى وجاهة الأدلة وبعدم قبول الإشاعات وبموثوقية الأدلة وسلامتها، وهي مبادئ قد تنطبق جميعها بشكل خاص على الأدلة الإلكترونية. وسلَّطت بلدان عديدة الضوء على التحديات التي تقوم في إسناد الأعمال إلى الشخص المعين الذي يرتكبها، وعلّقت بأنَّ هذا الأمر غالبا ما يتوقَّف على الدليل الظرفي.

وتدل التحديات التي تواجه المحققين والمدّعين العامين المكلفين بإنفاذ القانون على أنَّ معدّلات "التقديم للعدالة" أدنى بالنسبة لمرتكبي الجريمة السيبرانية. ولوحظ أنَّ عدد المشتبه بارتكابهم جرائم مسجّلة لدى

الشرطة في قضايا المواد الإباحية المتعلقة بالأطفال قابل للمقارنة بعدد المشتبه بارتكابهم جرائم جنسية أخرى. ولكنَّ عدد المشتبه بارتكابهم جرائم مسجّلة لدى الشرطة متعلقة بالنفاذ غير المشروع والاحتيال أو التزوير بواسطة الحواسيب لا يتجاوز 25 لكل 100 جريمة. ولم يتمكّن إلا عدد قليل جدا من البلدان من توفير البيانات بشأن الأشخاص الذين تمت مقاضاتهم أو إدانتهم. لكن إحصاءات الجريمة السيبرانية في بلد واحد أظهرت أنَّ نسبة الأشخاص الذين أُدينوا بارتكاب جريمة سيبرانية مسجّلة أقل بكثير من نسبة الأشخاص المدانين بارتكاب سائر الجرائم "التقليدية."

التعاون الدولي

أفادت البلدان التي أجابت عن الاستبيان بأنَّ 30 إلى 70 في المائة من أفعال الجريمة السيبرانية تشتمل على بعد عابر لحدود الوطن، ومن ثم تنطوي على مسائل متعلقة بالتحقيقات العابرة للحدود، والسيادة، والولاية القضائية، والأدلة الواقعة خارج نطاق الولاية القضائية، ومتطلّب التعاون الدولي. وينشأ البعد عابر الحدود للجريمة السيبرانية عندما يكون للجريمة المعنية عنصر أو أثر مهم في إقليم آخر، أو عندما يكون أحد جوانب تنفيذ الجريمة قد تم في إقليم آخر. وينصّ القانون الدولي على عدد من الأسس المتعلقة بالولاية القضائية بشأن الأفعال المعنية، بما في ذلك أشكال الولايات القضائية المستندة إلى الإقليم والمستندة إلى الجنسية. وتوجد بعض هذه الأسس أيضا في الصكوك متعددة الأطراف المتعلقة بالجريمة السيبرانية. وفي حين ترى كل البلدان الأوروبية أنَّ قوانينها الوطنية توفّر إطارا كافيا لتجريم الأفعال التي تندرج في عداد الجريمة السيبرانية والمرتكبة خارج نطاق الولاية القضائية ولملاحقة مرتكبيها قضائيا، فقد أبلغ نحو ثلث إلى أكثر من نصف البلدان في مناطق أخرى من العالم عن عدم كفاية الأطر القائمة في هذا المجال. وفي بلدان عديدة، تجسد الأحكام فكرة أنَّه ليس من الضروري أن تقع "كل عناصر" الجريمة داخل البلد من أجل تأكيد ولايته القضائية الإقليمية. ويمكن تحديد الروابط الإقليمية بالإشارة إلى عناصر الفعل المعني أو آثاره، أو موقع النظم أو البيانات الحاسوبية المستخدمة في ارتكابه. وتجري عادة تسوية تنازع الولايات القضائية من خلال المشاورات الرسمية وغير الرسمية بين البلدان. ولا تكشف إجابات البلدان حاليا عن أي حاجة إلى أشكال إضافية من الولاية القضائية على بعد "فضاء إلكتروني" مفترض، فغالبا ما تكون أشكال الولاية القضائية المستندة إلى الإقليم والمستندة إلى الجنسية قادرة دائما على ربط الجريمة السيبرانية المرتكبة ربطا كافيا بدولة واحدة على الأقل.



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 105. (ع=56، ن=221)

وتشمل أشكال التعاون الدولي تسليم المطلوبين وتبادل المساعدة القانونية والاعتراف المتبادل بالأحكام الأجنبية والتعاون غير الرسمي بين أجهزة الشرطة. ونظرا لطبيعة الأدلة السيبرانية التي تتسم بسهولة زوالها وتغيّرها، يتطلّب التعاون الدولي في المسائل الجنائية المتعلقة بالجرائم السيبرانية اتخاذ الإجراءات في الوقت المناسب والتمكن من طلب تنفيذ إجراءات تحقيق متخصصة، مثل حفظ البيانات الحاسوبية. ويعد استخدام الأشكال التقليدية للتعاون الأسلوب الأكثر شيوعا للحصول على الأدلة خارج نطاق الولاية الإقليمية في قضايا الجريمة السيبرانية، حيث أبلغ أكثر من 70 في المائة من البلدان عن استخدام طلبات المساعدة القانونية المتبادلة الرسمية لهذا الغرض. وفي إطار هذا النوع من التعاون الرسمي، يستخدم حوالي 60 في المائة من الطلبات الصكوك الثنائية باعتبارها الأساس القانوني للتعاون. وتُستخدم الصكوك متعددة الأطراف في 20 في المائة من الحالات. وأُفيد بأنَّ الاستجابة للطلبات المعنية تستغرق أشهرا لكل من طلبات تسليم المطلوبين والمساعدة القانونية المتبادلة، وتطرح هذه الفترة الزمنية تحديات على صعيد جمع الأدلة الإلكترونية سريعة الزوال والتغيُّر. وأفاد 60 في المائة من البلدان في أفريقيا والأمريكتين وأوروبا، و20 في المائة من البلدان في آسيا وأوقيانوسيا عن وجود قنوات للطلبات العاجلة، غير أنَّ تأثيرها على زمن الاستجابة غير واضح. وأفاد ثلثا البلدان المجيبة تقريبا بأنَّ أساليب التعاون غير الرسمي ممكنة، لكن عددا قليلا من البلدان كان لديه سياسة لاستخدام مثل هذه الآليات. وتوفِّر المبادرات المتعلقة بالتعاون غير الرسمي وبتسهيله، كالشبكات العاملة على الدوام (24/7)، إمكانيات مهمة لتسريع الاستجابة، لكنها غير مستخدمة بشكل كافٍ، إذ اقتصر استخدامها على نحو ثلاثة في المائة من العدد الإجمالي لقضايا الجريمة السيبرانية التي تناولتها سلطات إنفاذ القانون في مجموعة البلدان المبلغة.

وقد صُمِّمت أساليب تعاون الرسمية وغير رسمية لإدارة عملية موافقة الدولة على إجراء سلطات إنفاذ القانون الأجنبية تحقيقات تؤثّر على سيادتها. غير أنَّ المحققين يطلعون باطراد، عن علم أو غير علم، على بيانات تندرج خارج إطار الولاية القضائية لبلدهم خلال عملية جمع الأدلة، دون الحصول على موافقة الدولة التي تقع فيها البيانات فعليا. وتحدث هذه الحالة، بصورة خاصة، بسبب تقنيات الحوسبة السحابية التي تنطوي على تخزين البيانات في مراكز بيانات متعددة في مواقع جغرافية مختلفة. ويصبح "موقع" البيانات، وإن أمكنت معرفته من الناحية التقنية، اصطناعيا أكثر فأكثر، إلى حد أنه كثيرا ما توجّه طلبات المساعدة القانونية المتبادلة التقليدية إلى البلد الذي يوجد فيه مقدّم الخدمات، بدلا من البلد الذي يقع فيه مركز البيانات فعليا. وقد تحصل سلطات إنفاذ القانون الأجنبية مباشرة على البيانات التي تتجاوز حدود ولايتها الإقليمية عندما يستخدم المحققون رابطا مباشرا قائما انطلاقا من جهاز المشتبه به، أو عندما يستخدم المحققون وثائق تفويض قانونية بالحصول على البيانات. وقد يحصل المحققون المكلفون بإنفاذ القوانين، في بعض الأحيان، على البيانات من مقدمي الخدمات خارج الولاية الإقليمية من خلال تقديم طلب مباشر غير رسمي، على الرغم من أنّ مقدّمي الخدمات يطلبون عادة مراعاة الأصول القانونية. ولكن هذه الحالات غير مشمولة على النحو المناسب في الأحكام القائمة بالنفاذ إلى البيانات "عبر الحدود" المنصوص عليها في اتفاقية مجلس أوروبا المتعلقة بالجريمة

السيبرانية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وذلك بسبب التركيز على "موافقة" الشخص الذي يتمتع بالسلطة القانونية لإفشاء البيانات، والمعرفة المفترضة لموقع البيانات وقت النفاذ إليها أو استلامها.

وقد يفضي هذا الوضع على صعيد التعاون الدولي إلى ظهور مجموعات من البلدان لديها الصلاحيات والإجراءات اللازمة لتتعاون فيما بينها، في حين تبقى هذه الصلاحيات والإجراءات محصورة، بالنسبة لجميع البلدان الأخرى، بالوسائل "التقليدية" للتعاون الدولي التي لا تأخذ في الاعتبار خصوصيات الأدلة الإلكترونية والطابع العالمي للجريمة السيبرانية. وهذا هو الحال بصفة خاصة فيما يتعلق بالتعاون في إجراءات التحقيق. ويعني عدم وجود نهج مشترك، بما في ذلك في إطار الصكوك الحالية متعددة الأطراف بشأن الجرايمة السيبرانية، أنَّ طلبات اتخاذ الإجراءات، مثل الحفظ العاجل للبيانات خارج البلدان الملزَمة دوليا بضمان مثل هذه الخدمة وتوفيرها عند الطلب، قد لا تُنفّذ بسهولة. ومن شأن إدراج هذه الصلاحية في مشروع اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني أن يحقّق بعض التقدُّم في سدّ هذه الثغرة. أما على الصعيد العالمي، فإنَّ التباين في نطاق الأحكام المتعلقة بالتعاون في الصكوك الثنائية ومتعددة الأطراف، وعدم فرض أجل ملزم للاستجابة للطلبات، وعدم الاتفاق على إتاحة النفاذ المباشر إلى البيانات التي توجد خارج الولاية القضائية، وتعدُّد شبكات سلطات إنفاذ القانون غير الرسمية، والتباين في ضمانات التعاون، أمور تمثل تحديات كبيرة في وجه التعاون الدولي الفعال فيما يتعلق بالأدلة الإلكترونية في المسائل الجنائية.

منع الجريمة السيبرانية

ينطوي منع الجريمة على استراتيجيات وتدابير تسعى إلى التقليل من احتمالات حدوث جرائم والحد من آثارها الضارة التي قد تلحق بالأفراد والمجتمع. وقد أفاد نحو 40 في المائة من البلدان المجيبة عن الاستبيان بأنَّ لديها قانونا وطنيا أو سياسة وطنية بشأن منع الجريمة السيبرانية. وهناك حاليا مبادرات قيد الإعداد في بلدان أخرى تبلغ نسبتها 20 في المائة. وأبرزت البلدان أنَّ الممارسات الجيدة في مجال منع الجريمة السيبرانية تتضمن نشر التشريعات، والقيادة الفعّالة، وتنمية القدرات على صعيد العدالة الجنائية وإنفاذ القانون والتعليم والتوعية، وإنشاء قاعدة معرفية قوية، والتعاون بين الحكومة والمجتمعات المحلية والقطاع الخاص وعلى الصعيد الدولي. وأبلغ أكثر من نصف البلدان عن وجود استراتيجيات بشأن الجريمة السيبرانية. وفي حالات عديدة، أُدرجت الاستراتيجيات الخاصة بالجريمة السيبرانية بشكل وثيق ضمن استراتيجيات للأمن السيبراني. وتتضمن حوالي 70 في المائة من جميع الاستراتيجيات الوطنية المبلّغ عنها مكوّنات بشأن زيادة الوعي والتعاون الدولي والقدرات في مجال إنفاذ القانون. ولأغراض التنسيق، يُبلغ في أغلب الأحيان عن وكالات إنفاذ القانون والملاحقة القضائية باعتبارها مؤسسات رائدة معنية بالجريمة السيبرانية.

وتظهر الدراسات الاستقصائية، بما في ذلك في البلدان النامية، أنّ معظم مستخدمي الإنترنت من الأفراد يتخذون حاليا الاحتياطات الأمنية الأساسية. وقد أشارت الحكومات وهيئات القطاع الخاص والمؤسسات الأكاديمية المجيبة عن الاستبيان إلى أهمية استمرار حملات زيادة الوعي العام، بما في ذلك حملات

التوعية بالتهديدات الناشئة، والحملات التي تستهدف جمهورا محددا، كالأطفال. ويكون تعليم المستخدمين أكثر فعالية عندما يقترن بنظم تساعدهم على تحقيق أهدافهم بطريقة آمنة. فإذا كانت التكلفة التي يتكبدها المستخدم أعلى من المنفعة المباشرة التي يحصل عليها، لن يتشجّع الأفراد بشكل كبير على اتّباع الإجراءات الأمنية. وأفادت كيانات القطاع الخاص أيضا بأنه يجب إدراج توعية المستخدمين والموظفين في نهج شامل للأمن. وتتضمن المبادئ الأساسية والممارسة السليمة المشار إليها المساءلة عن العمل في مجال التوعية وعن سياسات وممارسات تدبُّر المخاطر والقيادة على مستوى مجالس الإدارة وتدريب الموظفين. وقد أجرى ثلثا المجيبين من القطاع الخاص تقييما لمخاطر الجريمة السيبرانية، وأبلغ معظمهم عن استخدام تكنولوجيا الأمن السيبراني كالجدران النارية، وحفظ الأدلة الرقمية، واستبانة المحتوى، وكشف التسلل، والإشراف على النظم ومراقبتها. ولكن أُبديت شواغل لأنَّ الشركات الصغيرة ومتوسطة الحجم إمَّا أنها لا تتخذ خطوات كافية لحماية النظم، أو تتصور بشكل خاطئ أنها لن تُستهدف.

وتؤدي الأطر التنظيمية دورا مهما في منع الجريمة السيبرانية فيما يتعلق بالقطاع الخاص عموما وبمقدّمي الخدمات خصوصا. وقد اعتمد حوالي نصف البلدان قوانين لحماية البيانات تحدِّد المتطلبات اللازمة لحماية البيانات الشخصية واستخدامها. وتتضمن بعض هذه القوانين متطلبات محدَّدة خاصة بمقدّمي خدمات الإنترنت وغيرهم من مقدّمي خدمات الاتصالات الإلكترونية. ولئن كانت قوانين حماية البيانات تتطلب حذف البيانات الشخصية عندما لا تعود لازمة، فقد وضع بعض البلدان استثناءات لأغراض التحقيقات الجنائية، تُلزِم مقدّمي خدمات الإنترنت بتخزين أنواع معينة من البيانات لفترة زمنية محدَّدة. ولدى العديد من الدول المتقدمة أيضا قواعد تلزم المنظمات بإبلاغ الأفراد والجهات التنظيمية عن الانتهاكات المتعلقة بالبيانات. ويتحمّل مقدّمو خدمات الإنترنت عادة مسؤولية محدودة باعتبارهم "مجرّد قنوات" لمرور البيانات. وتزداد هذه المسؤولية في حال قيامهم بتعديل المحتويات المنقولة، كما تزداد أيضا عند علمهم بصورة فعلية أو بناءة، بنشاط غير قانوني. وتكون المسؤولية محدودة من جهة أخرى في حال مسارعتهم إلى اتخاذ الإجراءات اللازمة إثر إبلاغهم بنشاط غير قانوني. ولئن كانت تتوافر لمقدِّمي خدمات الإنترنت إمكانيات تقنية لفرز محتوى الإنترنت، فإنَّ فرض قيود على النفاذ إلى شبكة الإنترنت يتوقف على القدرة على التوقع وينبغي أن يكون متناسبا مع مستوى التهديد، وهما شرطان واردان في القانون الدولي لحقوق الإنسان الذي يحمي حقوق التماس المعلومات وتلقيها ونقلها.

وتتَّسم الشراكات بين القطاع العام والقطاع الخاص بأهمية أساسية لمنع الجريمة السيبرانية. وقد أفاد أكثر من نصف مجموع البلدان عن وجود هذه الشراكات. وتُقام هذه الشراكات على السواء بموجب اتفاقات غير رسمية وعلى أسس قانونية. وهيئات القطاع الخاص هي أكثر من يدخل في شراكات، تليها المؤسسات الأكاديمية، والمنظمات الدولية والإقليمية. وتُستخدم الشراكات غالبا من أجل تيسير تبادل المعلومات عن التهديدات والاتجاهات، وكذلك من أجل تنفيذ أنشطة وإجراءات وقائية في حالات محددة. وفي سياق بعض الشراكات بين القطاع العام والقطاع الخاص، أخذت كيانات القطاع الخاص بنهج استباقي للتحقيق في الجريمة

السيبرانية واتخاذ إجراءات قانونية بشأنها. وتُكمّل هذه الإجراءات تلك التي تتخذها سلطات إنفاذ القانون ويمكن أن تساعد في تخفيف الضرر على الضحايا. وتؤدي المؤسسات الأكاديمية مجموعة متنوعة من الأدوار في منع الجريمة السيبرانية، من خلال أمور منها تثقيف المهنيين وتدريبهم ووضع القوانين والسياسات والعمل على تطوير المعايير والحلول التقنية. وتستضيف الجامعات الخبراء في مجال الجريمة السيبرانية، وبعض الأفرقة المعنية بمواجهة الطوارئ الحاسوبية (CERTs)، ومراكز البحوث المتخصصة، وتيسّر ما يضطلعون به من أعمال.



الفصل الأول: الموصولية والجريمة السيبرانية

يتناول هذا الفصل تأثير ثورة الاتصال العالمية على الجريمة السيبرانية، ويحدد مدلول الجريمة السيبرانية باعتبارها أحد التحديات المعاصرة المتزايدة المُنْساقة من قِبَل مجموعة من العوامل الاجتماعية والاقتصادية الكامنة. ويطرح هذا الفصل تعريفات للجريمة السيبرانية، ويتضح أنه في حين أن هناك حاجة لوجود تعريفات محددة للأفعال الرئيسية للجريمة السيبرانية، إلا أن المفهوم الشامل لا يعتبر مناسبا باعتباره مصطلحا قانونيّا قائما بحد ذاته.

1-1 ثورة الموصولية العالمية

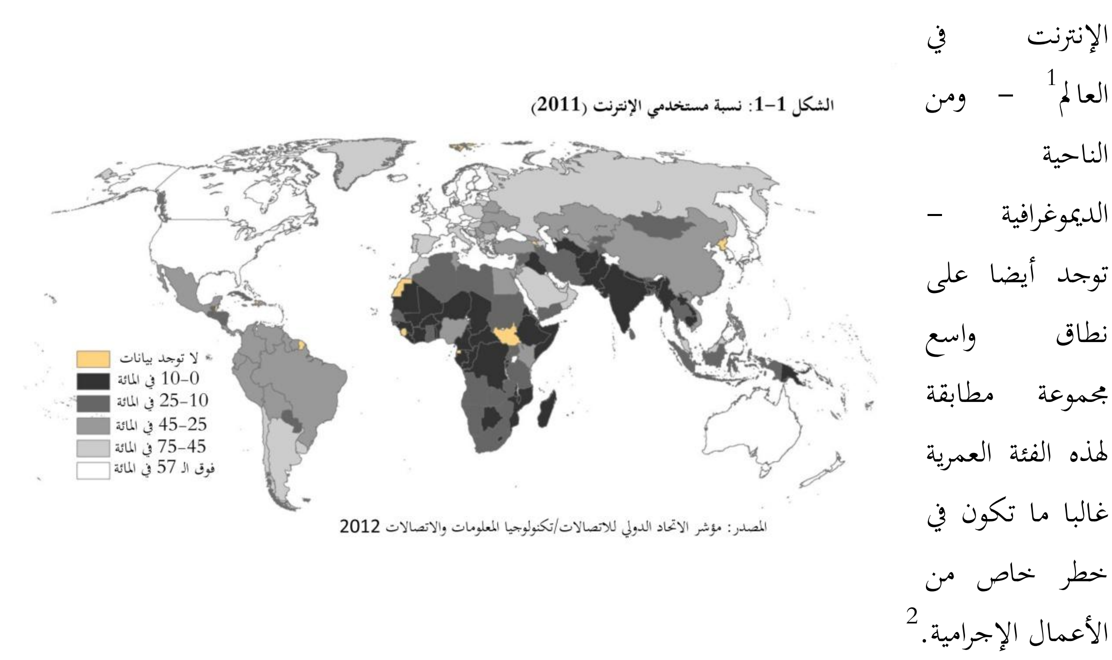
الاستنتاجات الرئيسية

- في عام 2011، كان عدد الموصولين بالإنترنت يعادل أكثر من ثلث مجموع سكان العالم
- يعيش أكثر من 60 في المائة من جميع مستخدمي الإنترنت في البلدان النامية، ولا يتجاوز عمر 45 في المائة من مجموع مستخدمي الإنترنت الـ25 عاما
- بحلول عام 2017، من المتوقع أن تناهز نسبة المشتركين في خدمة الإنترنت النقالة ذات النطاق العريض 70 في المائة من مجموع سكان العالم
- سيفوق عدد الأجهزة المتصلة بالشبكة ("الأشياء المتصلة بالإنترنت") عدد الناس بنسبة ستة إلى واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت
- في عالم الغد المتسم بالموصولية البالغة، سيصعب تصوُّر وقوع "جريمة حاسوبية" وربما أيِّ جريمة أخرى لا تنطوي على أدلة إلكترونية تتعلق بالموصولية بواسطة بروتوكول الإنترنت

في عام 2011، كان عدد الموصولين بالإنترنت لا يقل عن 2.3 بليون نسمة، أي ما يعادل أكثر من ثلث مجموع سكان العالم. وتتمتع الدول المتقدمة بمستويات أعلى (70 في المائة) من الدول النامية (24 في المائة) فيما يتعلق بالاتصال بشبكة الإنترنت، ومع ذلك، فإن العدد المطلق من مستخدمي الإنترنت في الدول النامية يفوق بالفعل عدد نظرائهم في الدول المتقدمة بِكَثِير، حيث بلغت نسبة مستخدمي الإنترنت في عام 2011 في الدول النامية 62 في المائة.

وتعتبر نسبة مستخدمي الانترنت من فئة صغار السن أعلى من فئة كبار السن، سواء في الدول المتقدمة أو الدول النامية؛ حيث تشكل الفئة العمرية دون سن الـ 25 عاما نسبة 45 في المائة من مستخدمي الإنترنت في العالم[1] – ومن الناحية الديموغرافية – توجد أيضا على نطاق واسع مجموعة مطابقة لهذه الفئة العمرية غالبا ما تكون في خطر خاص من الأعمال الإجرامية.[2]

الشكل 1-1: نسبة مستخدمي الإنترنت (2011)

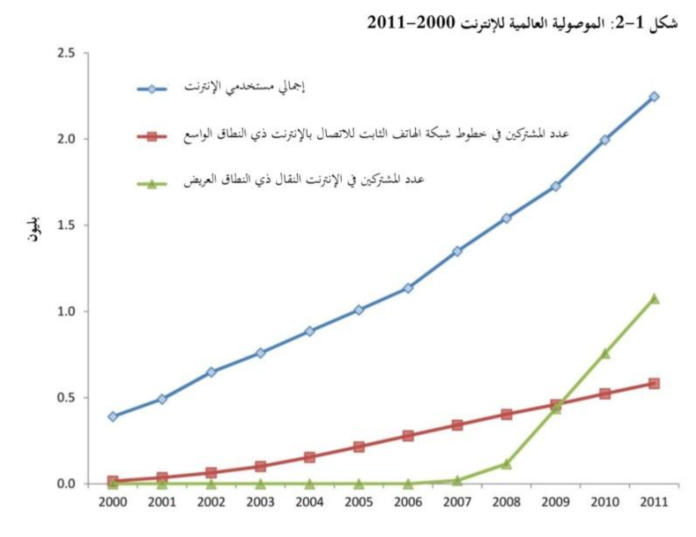


المصدر: مؤشر الاتحاد الدولي للاتصالات/تكنولوجيا المعلومات والاتصالات 2012

تزايد الاتصال بالإنترنت عبر الهاتف المحمول

يوجد – عالميا – ما يقرب من 1.2 مليار اشتراك في الإنترنت النقال ذي النطاق العريض، ويمثل ذلك؛ ضعف عدد خطوط شبكة الهاتف الثابت للاتصال بالإنترنت ذي النطاق الواسع، وهو ما يشكل نسبة 16 في المائة من سكان العالم.[3] ففي عام 2009، تجاوز حجم حركة بيانات الأجهزة المحمولة عالميا حجم حركة الاتصالات الصوتية المتنقلة، أما في عام 2011، فإن حركة بيانات

شكل 1-2: الموصولية العالمية للإنترنت 2000-2011



المصدر: مؤشر الاتحاد الدولي للاتصالات/تكنولوجيا المعلومات والاتصالات 2012

---

[1] الاتحاد الدولي للاتصالات، 2012. *قياس مجتمع المعلومات، قاعدة بيانات الاتصالات العالمية/ مؤشرات تكنولوجيا المعلومات*. أنظر أيضا: Moore, R., Guntupalli, N.T., and Lee, T., 2010. Parental regulation and online activities: دراسة العوامل التي تؤثر على إمكانيات الشباب لتصبح ضحية التحرش على الانترنت. *المجلة الدولية لعلم الجريمة السيبرانية*، 4 (1 و2): 685-698

[2] المفوضية الأوروبية، 2012. *Special Eurobarometer 390: Cyber Security Report*. See also Fawn, T. and Paternoster, *R., 2011. Cybercrime Victimization: An examination of individual and situational level factors*. *المجلة الدولية لعلم الجريمة السيبرانية*، 5 (1): 773-793، 782.

[3] الاتحاد الدولي للاتصالات، 2012. *قياس مجتمع المعلومات، قاعدة بيانات الاتصالات العالمية/ مؤشرات تكنولوجيا المعلومات*.

الأجهزة المحمولة عالميا قد شكلت نحو أربعة أضعاف حركة الاتصالات الصوتية المتنقلة.[1]

تُظهر أفريقيا والدول العربية نِسبا عالية – بصورة خاصة – في استعمال الإنترنت النقال ذي النطاق العريض بالمقارنة مع شبكة الهاتف الثابت للاتصال بالإنترنت ذي النطاق الواسع، ويعكس ذلك إطلاق سرعة عالية تقدر بـ 3 جيجا بالإضافة إلى شبكات وخدمات الهاتف المحمول في تلك المناطق، وذلك مَقْرُون بتزايد في استعمال الأجهزة المحمولة، بما في ذلك الهواتف الذكية وأجهزة الحاسوب اللوحي. وبحلول عام 2017، فإنه من المتوقع أن تغطي تكنولوجيا النظام العالمي لاتصالات الهاتف المحمول (GSM)/معدلات البيانات المعززة لتطوير النظام العالمي للتصالات (EDGE)[2] أكثر من 90 في المائة من سكان العالم، كما أنه من المتوقع وصول 85 في المائة من السكان إلى قنوات اتصال ذات ترددات عالية/وصول الحزم عالية السرعة (WCDMA/HSPA)[3] من تكنولوجيا الهاتف المحمول بسرعات تبدأ من 2 ميجابايت في الثانية. علاوة على ذلك؛ تشير التوقعات إلى أن عدد اشتراكات الإنترنت النقال ذي النطاق العريض سيبلغ خمسة بلايين بحلول عام 2017. ففي عام 2011، تجاوز عدد *الأجهزة* المتصلة بالشبكة – والتي يطلق عليها "الأشياء المتصلة بالإنترنت" – التعداد العالمي للسكان، وبحلول عام 2020، سيفوق عدد الأجهزة المتصلة بالشبكة عدد الناس بنسبة ستة إلى واحد، مما سيؤدي إلى تغيير المفاهيم الحالية للإنترنت.[4] وفي حين أن لدى الأشخاص المتصلين بالإنترنت في الوقت الحالي جهازا واحدا أو جهازين على الأقل متصلين بالإنترنت (عادة جهاز حاسوب وهاتف ذكي)، بيد أن هذا العدد من الأجهزة قابل للزيادة إلى سبعة أجهزة بحلول عام 2015.[5] وأخيرا، في "الأشياء المتصلة بالإنترنت" ستكون الأغراض، مثل الأجهزة المنزلية والسيارات والطاقة وعدادات المياه والأدوية، أو حتى المتعلقات الشخصية مثل الملابس، قابلة لتعيين "عنوان بروتوكول الإنترنت"، وتحديد أنفسهم والتواصل باستخدام تكنولوجيا مثل "التعرّف بواسطة التردد الراديوي (RFID)" و"اتصال المجال القريب (NFC)".[6]

الفجوة الرقمية المستمرة

يمكن بشكل واضح إبراز الفوارق في الدخول إلى الإنترنت من خلال تعيين الموقع الجغرافي لعناوين بروتوكول الإنترنت العالمية، ويعتبر هذا أحد التقديرات المناسبة للنطاق الجغرافي لشبكة الإنترنت. فبينما يرتبط الثقل النوعي لعناوين بروتوكول الإنترنت إلى حد كبير بالكثافة السكانية العالمية، إلا أن عددا من المواقع المأهولة بالسكان في البلدان النامية تظهر تواجدا غير كثيف في الاتصال بالإنترنت. وعلى الصعيد الآخر، تعتبر الفجوات الموجودة على – وجه الخصوص – في جنوب وشرق آسيا وأمريكا الوسطى وأفريقيا مثالا على الفجوة

---

[1] Ericsson, 2012. *Traffic and Market Report*

[2] تكنولوجيا النظام العالمي لاتصالات الهاتف المحمول/معدلات البيانات المعززة لتطوير النظام العالمي للتصالات.

[3] تقسيم شفرات الوصول المتعدد للنطاق العريض/ سرعة عالية لنقل حزم البيانات.

[4] الاتحاد الدولي للاتصالات، 2012، *حالة تقنية الاتصال السريع في عام 2012: تحقيق الإدماج الرقمي للجميع.*

[5] المفوضية الأوروبية، 2012. جدول *الأعمال الرقمي: مشاورات اللجنة بشأن قواعد اتصال الأجهزة لاسلكيا-الأشياء المتصلة بالإنترنت.*

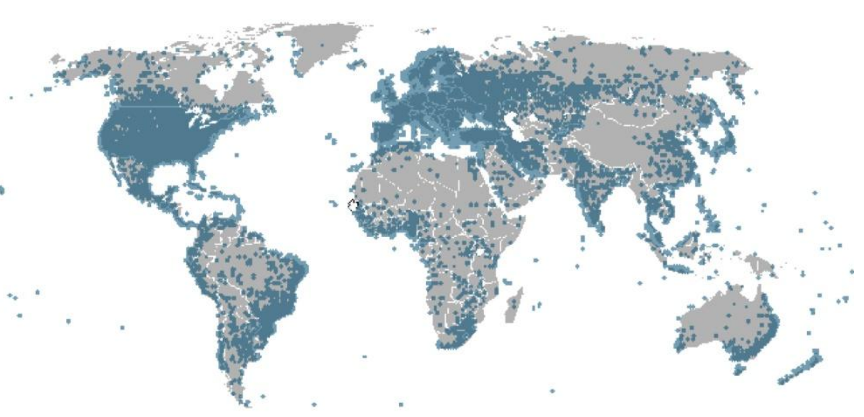
متاح عل الرابط التالي: http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=IoTGovernance

[6] التعرّف بواسطة التردد الراديوي واتصال المجال القريب.

الرقمية الحالية. ففي منتصف عام 2012، تبين أن عدد 341 مليون شخص في أفريقيا وجنوب الصحراء الكبرى يعيشون خارج نطاق 50 كليو متر مربع من شبكة ألياف بصرية أرضية، أي عدد يفوق عدد سكان الولايات المتحدة الأمريكية.[1]

كما لاحظت لجنة النطاق العريض المعنية بالتنمية الرقمية التي أنشأها الاتحاد الدولي للاتصالات واليونسكو أن المناطق غير المتصلة بالإنترنت تفقد إمكانات غير مسبوقة من الفرص الاقتصادية والرعاية الاجتماعية. ويقدر البنك الدولي أن زيادة انتشار خدمات النطاق العريض بنسبة 10 في المائة، يمكن أن يعود بالزيادة في نمو الناتج المحلي الإجمالي في البلدان منخفضة ومتوسطة الدخل بنسبة تصل في المتوسط إلى 1.38 في المائة.[2] كما تبين أن لدى النطاق العريض المتنقل تأثيرا أكبر على نمو الناتج المحلي الإجمالي من النطاق العريض الثابت، وذلك من خلال الحد من أوجه القصور التي قد تعتري الخدمة[3]. وأخيرا، إلى ما هو أبعد من أهداف النمو الاقتصادي، فإنه يمكن من خلال الاتصال بالإنترنت الحصول على خدمات حيوية من على بعد، بما في ذلك التعليم، والرعاية الصحية، والحوكمة الإلكترونية.

الشكل 1-3: تحديد الموقع الجغرافي لبرتوكولات الإنترنت (2012)



المصدر: مكتب الأمم المتحدة المعني بالمخدرات والجريمة/ MaxMind GeoCityLite.

دور القطاع الخاص

يمتلك القطاع الخاص جزءا كبيرا من البنية التحتية للإنترنت فضلا عن تشغيلها. ويتطلب وصول الإنترنت عدة أمور منها؛ بنية تحتية "خاملة" من الخنادق، والقنوات، والألياف البصرية، ومحطات الاتصالات المتنقلة، وأجهزة بث فضائي "قمر صناعي". كما يتطلب أيضا، بنية تحتية "فعالة" من المعدات الإلكترونية،

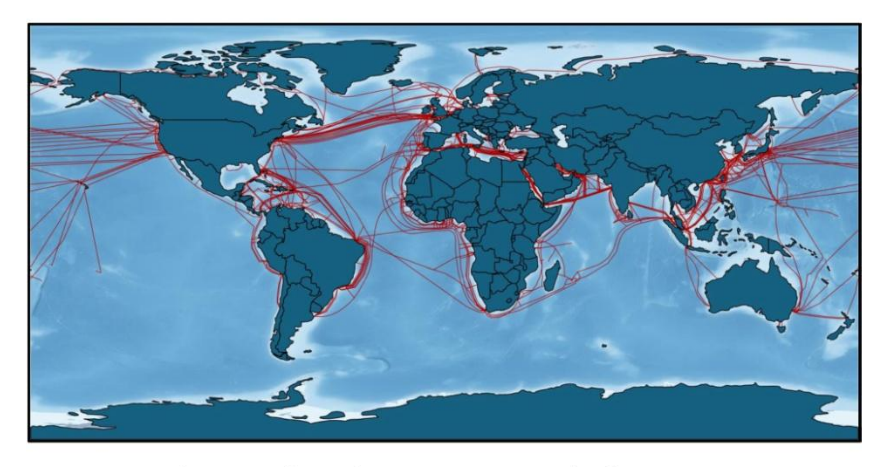
[1] منظمة الكومنولث للاتصالات، 2012. *تأثير العوامل الاقتصادية والاجتماعية للإنترنت ذي النطاق العريض في أفريقيا جنوب الصحراء الكبرى: ميزة الأقمار الصناعية.*

[2] البنك الدولي، 2009. *المعلومات والاتصالات من أجل التنمية: توسيع نطاق الوصول وزيادة التأثير.*

[3] البنك الدولي، 2012. *المعلومات والاتصالات من أجل التنمية: تعظيم الاستفادة من الهاتف المحمول.*

وطبقة من خدمات المحتوى وتطبيقات،[1] علاوة على شبكة كبيرة وعالمية من مزودي خدمات الإنترنت مثل: AT&T وNTT Communications وTelefonica, Sprint وVerizon، وكذلك امتلاك، أو تأجير، شبكة ألياف بصرية عالية القدرة على النقل عبر القارات وداخل القارة نفسها (حيث يعتبر ذلك العمود الفقري للإنترنت)، بالإضافة إلى البنية التحتية الأساسية للإنترنت، مثل المحولات والموجهات. ويتم توصيل شبكات مزودي خدمة الإنترنت بشكل ثنائي على حد سواء، وعند نقاط مركزة (يطلق عليها نقاط تبادل الإنترنت). وتتفاوض الشبكات الرئيسية فيما بينها (اتفاقات الندية) حيث توافق كل شبكة على نقل حركة الشبكة الأخرى، مما يتيح تقديم اتصالات عالمية سريعة لعملائها، كما تحمل أيضا البيانات المدفوعة للشبكات غير النظيرة. وتعمل شركات الهاتف المحمول، ومقدمو خدمات الإنترنت المحلية، وملاك أو مديرو الشبكات الخلوية، والكابلات المحلية على نقل الإنترنت من (الكيلومتر الأخير) الخادم إلى أجهزة الحاسوب المكتبية والمحمولة. ويحتوي المرفق الرابع لهذه الدراسة على مزيد من التفاصيل حول البنية التحتية للإنترنت.

الشكل 1–4: الكابلات البحرية العالمية



المصدر: بيانات مكتب الأمم المتحدة المعني بالمخدرات والجريمة من /http://www.cablemap.info

وبينما تسعى شركات عالمية إلى بناء قواعد واسعة في مجال الأعمال التجارية، وتحقيق أقصى قدر من الكفاءة والعائد، على الاستثمار في البنية التحتية، شهدت السنوات الأخيرة تقاربا بين التكنولوجيات التقليدية للمعلومات المحددة وتكنولوجيات الاتصالات، وخدمات شبكة الإنترنت.[2] وتقوم شبكات الاتصالات بتطوير جميع بيانات شبكات برتوكولات الإنترنت، مع منتجات موحدة وتبسيط الترابط، كما أن زيادة مساحة التخزين والحوسبة السحابية ستمكّن من تقديم نفس الخدمات والمحتوى المقدم للمستخدم إلى أي مستخدم لجهاز آخر، سواء كان الجهاز المستعمل هاتفا نقالا، أو حاسوبا مكتبيا أو لوحيا.

تكنولوجيا برتوكولات الإنترنت تقلل بصفة عامة تكلفة تشغيل الشبكة التجارية. ومع ذلك، فإن تكلفة النطاق الترددي الدولي لاتزال تختلف إلى حد كبير، وهذا يعتمد على مرونة العرض والطلب. وإلى أن

---

[1] الاتحاد الدولي للاتصالات، 2012. *حالة تقنية الاتصال السريع في عام 2012: تحقيق الإدماج الرقمي للجميع.*

[2] المنتدى الاقتصادي العالمي، 2012. التقرير الدولي لتقنية المعلومات 2012: *Living in a Hyper connected World*

يصبح الكابل البحري للساحل الأفريقي إلى أوروبا يعمل بكل طاقته، فإن هناك – على سبيل المثال – دولا في غرب أفريقيا لاتزال مثقلة ببعض من التكلفة الأعلى في العالم للموصولية بشبكة الإنترنت، ويرجع ذلك للاعتماد الحصري على عرض النطاق الترددي للأقمار الصناعية التجارية.[1]

هذا، ويمكن مقارنة تَطَوّر بنية الإنترنت التحتية بتنمية البنية التحتية للطرق والسكك الحديدية والكهرباء والتي تعتمد على استثمارات القطاع الخاص والبناء والصيانة، إلا أن هذا التطور يخضع إلى تنظيم وتحفيز الحكومات الوطنية. وفي نفس الوقت، غالبا ما يقود القطاع الخاص تنمية الإنترنت. فالعمل مع القطاع الخاص؛ يساعد الحكومات على تقديم منظومة لإدارة القطاع العام وتيسير عملية تطوير شبكة الإنترنت من خلال الاستثمار المباشر في البنية التحتية والخدمات من خلال وضع سياسات عملية تشجع المنافسة وتزيل معوقات الاستثمار، وأيضا من خلال تقديم حوافز للشركات التي تضطلع بتوزيع خدمات الإنترنت.[2]

2-1 الجريمة السيبرانية المعاصرة

الاستنتاجات الرئيسية:

- تعتبر الجرائم ذات الصلة بالحاسوب ظاهرة راسخة، إلا أن تطور الجريمة السيبرانية المعاصرة يرتبط ارتباطا لا انفصام له بنمو الموصولية العالمية
- تركز –اليوم– أنشطة الجريمة السيبرانية على الاستفادة من *عولمة* تكنولوجيا المعلومات والاتصالات لارتكاب أعمال إجرامية *عبر الحدود الوطنية*
- يرتكب بعض من الجريمة السيبرانية باستخدام تطبيقات قائمة بذاتها أو أنظمة حاسوب مغلقة، وإن كان ذلك بدرجة أقل تواترا بكثير

بالإضافة إلى المنافع الاقتصادية والاجتماعية لتكنولوجيا الكمبيوتر والإنترنت –كما هو الحال مع الوسائل الأخرى التي تعزز قدرات التفاعل البشري– إلا أنه يمكن استخدامهما في الأنشطة الإجرامية. وبينما تعتبر جرائم الحاسوب أو الجرائم ذات الصلة بالحاسوب ظاهرة راسخة نسبيا، إلا أن العامل الأصيل في الجريمة السيبرانية المعاصرة يتجسد في نمو الموصولية العالمية للإنترنت.

بدأت كثير من الدول منذ عام 1960 بالاعتراف بأن الأفعال المتصلة بالحواسيب، بما في ذلك؛ إلحاق الضرر المادي بأنظمة جهاز الحاسوب والبيانات المخزنة،[3] والاستخدام غير المأذون به للنظم الحاسوبية،

---

[1] منظمة الكومنولث للاتصالات، 2012. *تأثير العوامل الاقتصادية والاجتماعية للإنترنت ذي النطاق العريض في أفريقيا جنوب الصحراء الكبرى: ميزة الأقمار الصناعية.*

[2] المنتدى الاقتصادي العالمي، 2012. *التقرير الدولي لتقنية المعلومات 2012: Living in a Hyper connected World*

[3] فيما يتعلق بالتحديات ذات الصلة، أنظر:

والتلاعب بالبيانات الإلكترونية،[1] وأعمال الاحتيال المرتكبة بواسطة الحاسوب،[2] وقرصنة البرمجيات،[3] هي أفعال إجرامية.

في عام 1994، ذُكر في دليل الأمم المتحدة لمنع الجريمة المتصلة بالحواسيب ومكافحتها أنَّ من قبيل الأنواع الشائعة من جرائم الحاسوب؛[4] ارتكاب أعمال الاحتيال الحاسوبي، والتزوير الحاسوبي، وإتلاف أو إدخال تعديلات على بيانات أو برامج الحاسوب، والاستخدام غير المأذون به للنظم الحاسوبية والخدمات، والنسخ غير المرخص لبرامج الكمبيوتر المحمية قانونيا.

وفي وقت مبكر من عام 1979، أقر البعد *الدولي* لجرائم الحاسوب والتشريعات الجنائية ذات الصلة بأن مثل هذه الأفعال تعتبر في كثير من الأحيان جرائم محلية، حيث ترتكب باستخدام تطبيقات قائمة بذاتها أو أنظمة الكمبيوتر المغلقة. وفي الفترة من 11–13 كانون الأول/ديسمبر 1979، أكد عَرْض بشأن الاحتيال الحاسوبي في الندوة الثالثة التي عقدتها منظمة الإنتربول بشأن الاحتيال الدولي، على أن: "*جريمة الحاسوب ذات طبيعة دولية، ويرجع ذلك إلى؛ الزيادة المطردة للاتصالات بين مختلف الدول عبر الهواتف والأقمار الصناعية وما إلى ذلك*".[5]

إن المفهوم الأساسي الذي يحمله لُبّ الجريمة السيبرانية اليوم لايزال مُحَدَّدا بإمكانية استخدام الفكرة التي تتناول *عولمة* تكنولوجيا المعلومات والاتصالات في ارتكاب أعمال إجرامية *عبر الحدود*.

وقد تمتد هذه الأفعال لتشمل كافة الجرائم ذات الصلة بالحاسوب على النحو المذكور أعلاه، بالإضافة إلى العديد من الأفعال الأخرى مثل تلك المتعلقة بمحتوى الحاسوب أو الإنترنت،[6] أو الأفعال ذات الصلة بالحاسوب لتحقيق مكاسب شخصية أو مالية.[7] وعلى النحو المبيّن في هذا الفصل، فإن هذه الدراسة لا "تعرّف" الجريمة السيبرانية المعاصرة على هذا النحو، بل بالأحرى تصفها كقائمة من الأفعال التي تشكل جريمة سيبرانية. ومع ذلك؛ فمن الواضح أن التركيز في هذه الدراسة ينصب على سوء استخدام تكنولوجيا المعلومات والاتصالات من منظور عالمي. وأبلغ أكثر من نصف عدد البلدان المجيبة عن الاستبيان، على سبيل المثال، أن ما بين 50 و100 في المائة من أعمال الجريمة السيبرانية التي واجهتها الشرطة تشتمل على عنصر *عابر للحدود*

Slivka, R.T., and Darrow, J.W., 1975. Methods and Problems in Computer Security. *Rutgers Journal of Computers and Law,* 5:217

[1] الكونجرس الأمريكي، 1977. مشروع القانون الاتحادي لأنظمة الحاسوب 1766، الكونجرس 95، الدورة الأولى.
123 Cong. Rec. 20, 953 (1977).

[2] Glyn, E.A., 1983. Computer Abuse: The Emerging Crime and the Need for Legislation. Fordham Urban Law Journal, 12(1):73-101.

[3] Schmidt, W.E., 1981. Legal Proprietary Interests in Computer Programs: The American Experience. Jurimetrics Journal, 21:345.

[4] الأمم المتحدة، 1994. *دليل الأمم المتحدة لمنع الجريمة المتصلة بالحواسيب ومكافحتها.*

[5] الإنتربول، 1979. *الندوة الثالثة التي عقدها الإنتربول بشأن الاحتيال الدولي، باريس، 11–13 كانون الأول/ديسمبر 1979.*

[6] بما في ذلك، الأفعال التي تتعلق بالحاسوب وتنطوي على العنصرية أو كراهية الأجانب، أو استغلال الحاسوب في أعمال تتعلق بإنتاج أو توزيع أو حيازة مواد إباحية تتعلق باستغلال الأطفال جنسيا.

[7] بما في ذلك، جرائم الهوية المرتبطة بالحاسوب، وحقوق الطبع والنشر المتعلقة بالحاسوب، وجرائم استغلال العلامات التجارية.

الوطنية.[1] ووصف المجيبون على الاستبيان الجريمة السيبرانية بأنها "*ظاهرة عالمية*"، وذكروا أن "*التواصل عبر الإنترنت ينطوي دائما على أبعاد دولية أو عابرة للحدود الوطنية*".[2]

ولا يستبعد التركيز على الموصولية العالمية للإنترنت الجرائم التي تنطوي على استخدام تطبيقات قائمة بذاتها أو أنظمة حاسوب مغلقة من نطاق الجريمة السيبرانية.[3] ومن الأمور المثيرة للاهتمام في هذا الصدد، تحديد المسؤولين عن إنفاذ القانون في الدول المتقدمة نسبة عالية إجْمالا من الجريمة السيبرانية التي تشتمل على عنصر عابر للحدود الوطنية، في حين أن نظراءهم في الدول النامية إتجه إلى تعيين نسبة أقل من ذلك بكثير تقدر بـ 10 في المائة في بعض الحالات.[4] فمن ناحية، قد يشير هذا إلى أن مرتكبي الجريمة السيبرانية في الدول النامية يستهدفون بصورة أكبر الضحايا المحليين و(ربما باستخدام التطبيقات القائمة بذاتها) أنظمة الحاسوب المحلية. ومن ناحية أخرى، يمكن أن يكون الأمر أيضا، أنه نظرا للتحديات الماثلة أمام القدرات، فإن تحديد مقدمي الخدمات الأجانب أو الانخراط معهم من قبل أجهزة إنفاذ القانون في الدول النامية، أو التعرف على الضحايا المحتملين المرتبطين بالحالات الوطنية يكون أقل كثيرا.

ومع ذلك؛ يجب التسليم بأن واقع التواصل العالمي للإنترنت يعتبر الركن المركزي للجريمة السيبرانية المعاصرة، ولاسيما في المستقبل. وفيما يتعلق بالفضاء السيبراني ونمو حركة مرور معلومات برتوكولات الإنترنت[5]، فقد لُوحظ أن حركة مرور المعلومات من الأجهزة اللاسلكية تتجاوز حركة المرور من الأجهزة السلكية، وبتشكل المزيد من حركة مرور المعلومات عبر الإنترنت من أجهزة غير أجهزة الحاسوب الشخصي، قد يصبح من الصعب تصوّر وقوع جرائم تتصل بالحاسوب بدون وجود التواصل العالمي باستخدام بروتوكولات الإنترنت. ونظرا للطبيعة الشخصية الخاصة لأجهزة الهاتف المحمول وظهور الموصلية المنزلية لبروتوكولات الإنترنت أو الأمتعة الشخصية، فإن ذلك يعني أن عمليات توليد البيانات الإلكترونية والإرسال، أو جزء منها، هو نتاج كل عمل بشري تقريبا، سواء كان ذلك العمل قانونيا أو غير قانوني.

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 83.

[2] المرجع نفسه.

[3] ترى بعض الاتجاهات أن الجريمة السيبرانية ذات مفهوم أضيق من الجريمة ذات الصلة بالحاسوب، بِقَدْرِ ما تتطلب الجريمة السيبرانية وجود شبكة حاسوب – وبذلك تستبعد الجرائم المرتكبة التي استخدم فيها أنظمة حاسوب مستقلة بذاتها. في حين أن التركيز على سمة الموصولية، فإن هذه الدراسة لا تستبعد الجرائم التي تنطوي على استخدام أنظمة حاسوب قائمة بحد ذاتها أو مغلقة، من نطاق الجريمة السيبرانية. ومن ثم؛ فإن مصطلح "جريمة سيبرانية" يستخدم لوصف مجموعة من الجرائم بما في ذلك جرائم الحاسوب التقليدية، فضلا عن جرائم شبكة الإنترنت.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 83.

[5] In 2016 the gigabyte equivalent of all movies ever made will cross global IP networks every 3 minutes. Cisco, 2012. *Cisco Visual Networking Index, 2011-2016*.

3-1 الجريمة السيبرانية باعتبارها تحديا متزايدا

الاستنتاجات الرئيسية:

- نظرا للصعوبات التي تنشأ عن محاولة تعريف الجريمة السيبرانية وتحديد ماهيتها، فإن الإحصاءات المقارنة عبر الحدود الوطنية بشأن الجريمة السيبرانية قليلة بكثير إذا ما قورنت بأنواع الجرائم الأخرى
- ترى أجهزة إنفاذ القانون المجيبة عن الاستبيان الخاص بهذه الدراسة تزايد مستويات الجريمة السيبرانية على الصعيد العالمي، حيث يسعى كل من الجناة: الأفراد أو الجماعات الإجرامية المنظمة إلى استغلال الفرص الجديدة للحصول على الربح وتحقيق مكاسب شخصية
- تعتبر الجريمة السيبرانية محور اهتمام الجمهور، وذلك بسبب تزايد التغطية الإعلامية لقضايا الجريمة السيبرانية، وقضايا الأمن السيبراني، والأخبار الأخرى المتعلقة بالسيبرانية
- تقدم نظريات علم الإجرام والمناهج الاجتماعية والاقتصادية تفسيرات محتملة بشأن تزايد أنشطة الجريمة السيبرانية في الآونة الأخيرة
- شهدت بلدان عديدة زيادة هائلة في الموصولية العالمية في وقت يتّسم بتحوّلات اقتصادية وديمغرافية وبتزايد التفاوت في الدخل وتقييد الإنفاق في القطاع الخاص وانخفاض السيولة المالية

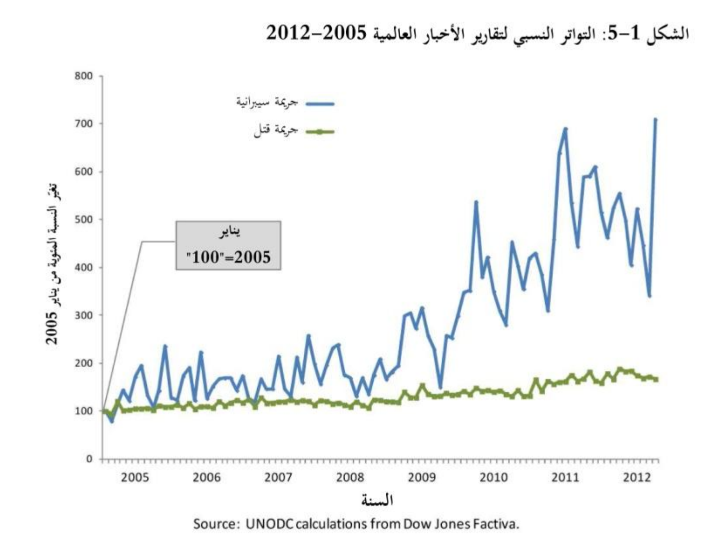
يمثل تزايد وجود الموصولية العالمية في كل مكان في جميع الأوقات خطرا جسيما سيزيد من معدلات الجريمة السيبرانية، وبينما توجد صعوبة في الحصول على إحصاءات موثوق بها، إلا أن العديد من الدول المجيبة عن الاستبيان الخاص بهذه الدراسة أشارت إلى أن الجريمة السيبرانية تمثل تحديا متزايدا، ويعتبر ذلك وجهة نظر مقبولة حيث أعطت العوامل الإجرامية والاجتماعية والاقتصادية بعدا أساسيا. ذكرت إحدى الدول الأوروبية المجيبة عن الاستبيان الخاص بهذه الدراسة أنه: "*من المتفق عليه أن الجريمة السيبرانية آخذة في التزايد بشكل كبير في ظل صلاحيات محدودة للرقابة عليها، وذلك في ضوء البحث والإحصاءات المقدمة في الغالب من القطاع الخاص أو المؤسسات الأكاديمية*".[1] وفي عام 2010، أشار إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية، المرافق لقرار الجمعية العامة 230/65، إلى أنَّ: "*تطوّر تكنولوجيات المعلومات والاتصالات وزيادة استخدام الإنترنت يهيئان فرصا جديدة للمجرمين وييسّران تنامي الجريمة*".[2]

[1] إستبيان دراسة الجريمة السيبرانية، السؤال رقم 84.
[2] *إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية*، المرافق لقرار الجمعية العامة للأمم المتحدة 230/65، A/Res/65/230 بشأن *مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية*، 1 نيسان/أبريل 2011، صفحة رقم 39.

بسبب التحديات الجسيمة في تحديد أبعاد ماهية الجريمة السيبرانية، فإن الإحصاءات المقارنة عبر الحدود الوطنية بشأن الجريمة السيبرانية قليلة بكثير إذا ما قورنت بأنواع الجرائم الأخرى.[1] ويتناول المرفق الثاني لهذه الدراسة الأساليب المنهجية الحالية لقياس الجريمة السيبرانية، ويعرض بعضا من الإحصاءات القليلة المتاحة.

لقد برزت بشكل واضح في السنوات الخمس الماضية على وجه الخصوص، مسألة الجريمة السيبرانية وتصدرت المناقشات العامة، بما في ذلك في البلدان النامية. وفي هذا الصدد، يكشف البحث في وكالات الأنباء العالمية عن ماهية مصطلح "الجريمة السيبرانية" ومصطلح "القتل"، باللغات الست للأمم المتحدة، عن تزايد نسبي كبير في المراجع الإخبارية المتواترة للجريمة السيبرانية، بالمقارنة مع المراجع الإخبارية لجريمة القتل. هذا، وقد تزايدت، ما بين عامي 2005 و2012، الجريمة السيبرانية بنسبة تصل إلى 600 في المائة، في حين وصلت النسبة في حالة جريمة القتل إلى 80 في المائة تقريبا،[2] بيد أن هذه القياسات لا تتعلق مباشرة بالأفعال الأساسية للجريمة السيبرانية. ومع هذا، يمكن أن تعكس هذه القياسات "النشاط" العالمي العام بشأن الجريمة السيبرانية، بما في ذلك تقارير وسائل الإعلام بشأن المبادرات الحكومية والإجراءات المضادة لهذه الجرائم.

الشكل 1-5: التواتر النسبي لتقارير الأخبار العالمية 2005-2012



Source: UNODC calculations from Dow Jones Factiva.

تعكس وجهات نظر الموظفين المكلفين بإنفاذ القانون أيضا إجماعا على أن مستويات الجريمة السيبرانية آخذة في التصاعد. وعند سؤالهم بشأن رصد اتجاهات الجريمة السيبرانية في بلدانهم على مدى السنوات الخمس الماضية؛ أجاب جميع الموظفين المكلفين بإنفاذ القانون في 18 دولة في أفريقيا ودول الأمريكتين بأن الجريمة السيبرانية تتزايد أو آخذة في التصاعد بقوة،[3] بينما يرى الموظفون المكلفون بإنفاذ القانون في أوروبا وآسيا وأوقيانوسيا أن الجريمة السيبرانية تتزايد ولكن لا تتصاعد بقوة، في حين أن عددا محدودا من دول أوروبا اعتبرها ظاهرة راسخة.[4]

---

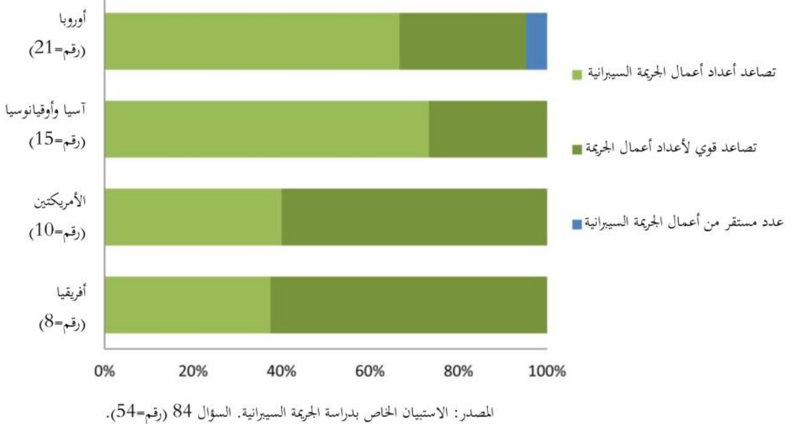
[1] اللجنة الإحصائية للأمم المتحدة، 2012. *تقرير المعهد الوطني المكسيكي للإحصاء والجغرافيا بشأن إحصاءات الجريمة*، مذكرة من الأمين العام للأمم المتحدة E/CN.3/2012/3، 6 كانون الأول/ديسمبر 2011.

[2] UNODC calculations from Dow Jones Factiva

[3] الاستبيان الخاص بدراسة الجريمة السيبرانية. السؤال رقم 84. Due to variable preparation and release times for official statistics, this may refer to the time period of 2007 to 2011 or 2006 to 2010 ('the last five years')

[4] المرجع السابق.

أشار الموظفون المكلفون بإنفاذ القانون إلى مجموعة من الأفعال التي تشكل الجريمة السيبرانية الآخذة في التصاعد؛ ويدخل في نطاق هذه الأفعال؛ الاحتيال الحاسوبي وانتحال الشخصية،



الشكل 1-6: رصد اتجاهات الجريمة السيبرانية من قِبل أجهزة إنفاذ القانون 2007–2011

المصدر: الاستبيان الخاص بدراسة الجريمة السيبرانية. السؤال 84 (رقم=54).

وإنتاج أو توزيع أو حيازة مواد إباحية فيها استغلال جنسي للأطفال، ومحاولات التصيّد الاحتيالي، والاختراق غير المشروع لأنظمة الحاسوب، بما في ذلك القرصنة. ورجّح الموظفون المكلفون بإنفاذ القانون تصاعد مستويات الجريمة السيبرانية جزئيا إلى تزايد قدرة تقنيات عدم الكشف عن الهوية عند استخدام تكنولوجيا المعلومات والاتصالات، فضلا عن تنامي تسويق أدوات إساءة استخدام الحاسوب. ويتناول الفصل الثاني (الصورة العالمية) مزيدا من تحليل المعلومات المقدمة من الدول والقطاع الخاص بشأن اتجاهات مُحَدّدة من أعمال الجريمة السيبرانية والتهديد الذي يصاحبها.

العوامل الأساسية: النهج الاجتماعية والاقتصادية والإجرامية

يعتبر الرأي القائل بأن تكنولوجيا المعلومات والاتصالات وزيادة استخدام الإنترنت يهيئان فرصا جديدة للمجرمين وييسّران تنامي الجريمة؛ أمرا منطقيا ومقبولا من منظور علم الإجرام. وبينما يوجد عدد من النظريات المختلفة المفسّرة للظاهرة الإجرامية قابلة للتطبيق، إلا أنه من خلال تطبيق النظريات العامة للجريمة؛[1] يتضح أن واقع الجريمة السيبرانية يشكل "*نموذجا إجراميا جديدا وفريدا*"[2] يفرض تحديات على التطورات المتوقّعة، وعلى مكافحتها.

تستند إحدى أهم الافتراضات إلى أنَّ ظهور "الفضاء السيبراني" يوجِد ظواهر إجرامية جديدة تختلف اختلافا بيّنا عن وجود أنظمة الحاسوب ذاتها، وكذلك الفرص المباشرة لارتكاب الجرائم التي يتيحها الحاسوب. فداخل الفضاء السيبراني، قد يُظهر الأشخاص الاختلافات بين سلوكهم المطابق (مشروع) وسلوكهم المخالف (غير مشروع) بالمقارنة مع سلوكهم في العالم المادي. فمن الممكن، على سبيل المثال، أن يرتكب أشخاص

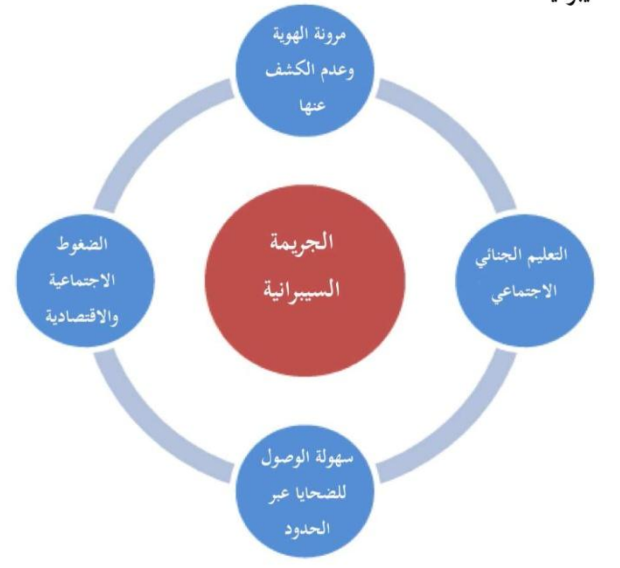
---

[1] *Koops, B.J., 2010. The Internet and its Opportunities for Crime. In: Herzog-Evans, M., (ed.) Transnational Criminology Manual. Nijmegen, Netherlands: WLP, pp.735-754.*

[2] Yar, M., 2005. The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology,* 2(4):407-427

جرائم في الفضاء السيبراني ما كان لهم أن يرتكبوها في الحيِّز المادي بحكم وضعهم ومكانتهم. وبالإضافة إلى ذلك؛ توفر المرونة وإمكانية اتخاذ هويات غير ثابتة، وإخفاء الهوية، وغياب الرادع حوافزَ على السلوك الإجرامي في الفضاء السيبراني.[1]

الشكل 1–7: إمكانية تحديد العوامل المرتبطة بتصاعد الجريمة السيبرانية



قد تقدم نظرية النشاط الإجرامي الاعتيادي (RAT)[2] أيضا فهما متعمقا للدوافع الكامنة وراء ارتكاب الجريمة السيبرانية. وتفترض نظرية النشاط الإجرامي الاعتيادي أنَّ مخاطر احتمال حدوث جريمة يزداد عندما تجتمع عدّة عناصر: (1) مجرم لديه دافع لارتكاب الجريمة، و(2) ضحية هي هدف ملائم، و(3) غياب الرقابة القوية.[3] وفي حالة الجريمة السيبرانية، يمكن للجناة أن يصلوا إلى أعداد كبيرة من الأهداف من خلال الوقت المتزايد الذي يقضونه على الإنترنت، بالإضافة إلى الاستعمال المتزايد للخدمات الإلكترونية المباشرة مثل الخدمات المصرفية، والتسوُّق، وشبكات التواصل الاجتماعي، والتشارك في الملفات، مما يجعل المستعملين عرضة لهجمات "التصيُّد الإلكتروني الاحتيالي" أو الاحتيال.[4] علاوة على ذلك، فإن ظهور الشبكات الاجتماعية على الإنترنت، بما في ذلك تويتر وفيسبوك، يوفر إطارا جاهزا من ملايين الضحايا المحتملين للغش أو الاحتيال. وفي حالة عدم قيام المستخدمين بضبط إعدادات الاتصال ليتمكنوا من التفاعل فقط مع شبكتهم الخاصة بهم من "الأصدقاء"، فإن مثل هذه الشبكات يمكن أن توفر عددا كبيرا من الضحايا المحتملين في كل مرة. هذا، ويميل الأشخاص أيضا إلى تنظيم ملامح شبكة التواصل الاجتماعي الخاصة بهم وفقا لاهتماماتهم وأماكنهم، مما يمكّن المجرمين من استهداف ضحايا ذوي أنماط سلوك معينة أو خلفيات محددة. بيد

---

[1] Jaishankar. K., 2011. Expanding Cyber Criminology with an Avant-Garde Anthology. *In:* Jaishankar, K., (ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour.* Boca Raton, FL: CRC Press, Taylor & Francis Group

[2] Kigerl, A., 2012. Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review,* 30(4):470-486, 470.

[3] المرجع السابق.

[4] للمزيد من المراجع والنظرة الشاملة، أنظر:

ibid. p.473; Hutchings, A., Hennessey, H., 2009. Routine activity theory and phishing victimization: Who got caught in the 'net'? *Current Issues in Criminal Justice,* 20(3):433-451; Pratt, T.C., Holtfreter, K., Reisig, M.D., 2010. Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3):267-296

أن هذه التدابير الرقابية التي توجد بالفعل، مثل برامج مكافحة الفيروسات ووجود مخاطر (ضئيلة نسبيا) للوقوع عرضة لإجراءات إنفاذ القانون، يمكن أن تكون غير كافية لردع الجناة المدفوعين بإغراء تحقيق أرباح كبيرة.

وفي هذا السياق، يُبرز البحث أيضا أن النظرية العامة للجريمة بشأن عدم ضبط النفس والقابلية لركوب المخاطر بغرض تحقيق مكاسب على المدى القصير، قد يسري على الأفعال التي يمكن تيسيرها أو تعزيزها من خلال الاتصالات الإلكترونية والإنترنت. بالإضافة إلى ذلك؛ فإن تعرّض الأفراد على الإنترنت لنماذج من السيبرانية الجنائية، والأقران أنفسهم يمكن أن يجعل منهم فئة أكثر عرضة للانخراط في الجرائم السيبرانية.[1] وقد يكون لنظرية "التعليم الاجتماعي" تطبيقات خاصّة عندما يتعلق الأمر بجريمة سيبرانية، حيث غالبا ما يحتاج المجرمون إلى تعلم تقنيات وإجراءات مُعَيّنة متعلقة بالحاسوب.[2] وفي ضوء تفاعل نظرية التعليم الاجتماعي والنظرية العامة للجريمة فإن هؤلاء الأشخاص الذين يعانون من عدم ضبط النفس قد يبحثون بنشاط عن أشخاص آخرين مماثلين لهم ويتجمعون معهم في البيئة الافتراضية بنفس الطريقة كما هو الحال في العالم الحقيقي. ففي الفضاء السيبراني، يمكن أن تحدث هذه العملية في إطار زمني قصير بشكل كبير وبامتداد جغرافي أوسع من ذلك بكثير.

تعتبر الموصولية عبر شبكة الإنترنت (online connectivity) وتعلّم الأقران بعضهم من بعض (peer-learning) بمثابة العنصر المركزي، على الأرجح، لانخراط عصابات الجريمة المنظمة في الجريمة السيبرانية، فعلى سبيل المثال، تيسِّر المنتديات الإلكترونية المسماة "قرصنة بطاقات الائتمان" أو "قراصنة بطاقات الائتمان" تبادل بيانات بطاقات الائتمان المسروقة. وقد بدأت منتديات قراصنة بطاقات الائتمان غالبا على شكل "جَمَاعَة" مع عدم وضوح هيكل للقيادة، حيث يسعى جناة الإنترنت للبحث عن بعضهم البعض، و"يلتقون" عبر الإنترنت لتبادل الخبرة وتقديم الخدمات غير المشروعة. ثم بدأت لاحقا منتديات قراصنة بطاقات الائتمان تتطور تصبح أشبه منها بعمليات "المحور" تتميز بدرجات أعلى من التنظيم الإجرامي.[3] وأخيرا، يمكن أن ييسّر استخدام مواقع شبكات التواصل الاجتماعي أشكالا من التواصل والموصولية بين الجماعات الإجرامية.[4]

---

[1] Holt, T.J., Burruss, G.W., Bossler, A.M., 2010. Social Learning and Cyber Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. *Journal of Crime and Justice*, 33(2):31-61.

[2] Skinner, W.F., Fream, A.M., 1997. A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, 34(4):495-518.

[3] BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. *Organised Crime in the Digital Age.*

[4] A number of Twitter feeds, for example, either purport to represent individuals associated with hacking groups such as Anonymous or Lulzsec, or the organizations themselves.

وهناك تطور أساسي آخر قد يسهم في دفع مستويات الجريمة السيبرانية يتمثل في وجود الموصولية العالمية في سياق ما يشهده العالم من تحولات اقتصادية وديمغرافية. فمن المتوقع، أن يتضاعف سكان المدن ليصل إلى 6.2 بليون نسمة بحلول عام 2050، أي أن 70 في المائة عدد سكان العالم المتوقّع سيصل إلى 8.9 بليون نسمة.[1] وذكر تقرير المخاطر العالمية الصادر عن المنتدى الاقتصادي العالمي في 2012، أن التفاوت في الدخل والإختلالات المالية الخطيرة والمتزايدة تشكل اثنين من المخاطر الخمسة الرئيسية التي سيشهدها العالم في عام 2012.[2] وتكشف بيانات مؤسسات جالوب لاستطلاعات الرأي، أنه مع بداية عام 2011 تأثر الناس – على مستوى العالم – من تَدَهْوُر مستويات المعيشة، مما أثار استياءهم نظرا للتفاوت الصارخ في الدخل.[3] ويُظهر البحث الذي أجراه مكتب الأمم المتحدة المعني بالمخدرات والجريمة أن العوامل الاقتصادية تلعب دورا هامّا في تطور اتجاهات الجريمة، حيث تم فحص 12 دولة من مجموع 15دولة، وأظهرت النماذج الإحصائية بعضا من الارتباط الشامل بين التغيرات الاقتصادية وثلاثة أنواع من الجرائم التقليدية في 12 دولة.[4]

شكل 1–8: التغيرات الاجتماعية والاقتصادية ووتيرة استخدام الإنترنت في أحد بلدان أوروبا الشرقية 2006–2011

المصدر: المكتب الإحصائي للجماعات الأوروبية ومؤشرات الاتحاد الدولي للاتصالات 2012

قد تلعب العوامل الاقتصادية والاجتماعية دورا هامّا في زيادة الجريمة السيبرانية، حيث يمكن أن يؤدي الضغط على مؤسسات القطاع الخاص لتقليل النفقات وخفض مستويات التوظيف، على سبيل المثال، إلى وجود ثغرات في مجال الأمن، وإتاحة الفرص للكشف عن نقاط الضعف التي تعتري تكنولوجيا المعلومات والاتصالات.[5] فإجبار الشركات على توظيف متعاقدين من خارج الشركة أو توظيف عمالة مؤقتة، أو أن يصبح الموظفون في حالة استياء من خفض رواتبهم، والخوف من فقد الوظيفة، كلها عوامل قد تزيد من الأعمال

---

[1] المنتدى الاقتصادي العالمي، 2012، *Outlook on the Global Agenda 2011*

[2] المنتدى الاقتصادي العالمي، تقرير المخاطر العالمية 2012.

[3] المرجع السابق، citing Credit Suisse Research Institute, 2011. *Global Wealth Report 2011*

[4] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2011، *رصد واقع الأزمة الاقتصادية على الجريمة*.

[5] BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. *Organised Crime in the Digital Age*

الإجرامية الفردية ومن نفوذ الجماعات الإجرامية المنظمة عبر المطلعين على شؤون الشركة.[1] ولقد عبرت بعض من الشركات المتخصّصة في الأمن السيبراني، بأن أحد التهديدات المحتملة أثناء فترات التراجع الاقتصادي تتمثل في الموظفين السابقين الذين قد تم تسريحهم لوجود فائض من العمالة،[2] كما ذكرت أيضا أن زيادة أعداد العاطلين عن العمل، أو تزايد أعداد الطلبة الخرجين الذين يعملون في وظائف غير مناسبة ولديهم مهارات حاسوبية يشكلون أحد الموارد الجديدة للجريمة المنظمة.[3]

ولا يقتصر دور العوامل الاجتماعية والاقتصادية في الجريمة السيبرانية على العالم المتقدم، بل يمتد تأثيرهما على قدم المساواة في سياق البلدان النامية. ففي أحد بلدان غرب أفريقيا، على سبيل المثال، تُظهر دراسات بشأن الخصائص الاجتماعية والديمغرافية لـ "*yahooboys*"[4] أن العديد من الطلبة الجامعيين يعتبرون الاحتيال عبر الإنترنت أحد الوسائل لكسب الرزق.[5] وتعتبر البطالة بصفة خاصة أحد العوامل الرئيسية لاستدراج الشباب إلى (*yahooboysim*).[6] وأظهرت دراسة في دولة أخرى في أفريقيا على نحو مماثل، أن شباب الـ (*Sakawa*) كثيرا ما تستحوذ أعمال الاحتيال عبر الإنترنت على نشاطهم واهتماماتهم، مبررين ذلك؛ بأن هذه هي الوسيلة الوحيدة التي تمكنهم من البقاء على قيد الحياة في ظل غياب فرص العمل.[7]

يعتبر تتزايد الجريمة السيبرانية المعاصرة من الأمور الجديرة بالاهتمام نظرا لتأثيرها والتهديد المصاحب لها على مستويات متعددة. وردا على سؤال حول التهديد الذي يصاحب الجريمة السيرانية، أشار الموظفون المكلفون بإنفاذ القانون إلى مجموعة من التأثيرات، تشتمل على حقيقة مفادها أن بعضا من أعمال الجريمة السيبرانية تسبب تأثيرا كليّا فيما يتعلق بحجم الإيذاء والآثار التراكمية، ومثال على ذلك الاحتيال وانتحال الشخصية والتي تشكّل تهديدا لأنها من الجريمة السيبرانية الشائعة. ويستعرض الفصل الثاني (الصورة العالمية) من هذه الدراسة نطاق الأثر المالي للجريمة السيبرانية على الأفراد والشركات. فمثل هذه الأفعال قد توجِد أيضا موارد للجماعات الإجرامية المنظمة والتي يمكن أن تستخدم لدعم مزيد من ارتكاب الجرائم. الأفعال الأخرى

---

[1] المرجع السابق.

[2] McAfee, 2009. *Unsecured Economies: Protecting Vital Information*

[3] BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. *Organised Crime in the Digital Age*

[4] تصف الثقافة الفرعية *yahooboys* الشباب وبخاصة هؤلاء الذين يعيشون في المدن، والذين يستعملون الإنترنت في أعمال الاحتيال المتعلقة بالحاسوب، علاوة على التصيد الاحتيالي والغش.

للمزيد، أنظر:

Adeniran, A.I., 2011. Café Culture and Heresy of Yahooboyism. *In:* Jaishankar, K., (ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

[5] Adeniran, A.I., 2008. The Internet and Emergence of Yahooboys sub-Culture. *International Journal of Cyber Criminology*, 2 (2):368-381; and Aransiola, J.O., Asindemade, S.O., 2011. Understanding Cybercrime Perpetrators and the Strategies They Employ. *Cyberpsychology, Behaviour and Social Networking*, 14(12):759.

[6] المرجع السابق.

[7] Warner, J., 2011. Understanding Cybercrime: A View from Below. *International Journal of Cyber Criminology*, 5(1):736-749.

للجريمة السيبرانية، مثل تطوير أدوات حاسوب غير شرعية مسيئة، على الرغم من أنها نادرة جدا، إلا أنها تشكل تهديدا خطيرا، حيث قد تشكل الحوادث الفردية أضرارا جسيمة. وتوجد فئة ثالثة تتضمن جرائم تسبب ضررا للأفراد، مثل إنتاج مواد إباحية تستغل الأطفال، وتوزيعها من خلال الإنترنت.[1]

4-1 وصف الجريمة السيبرانية

الاستنتاجات الرئيسية:

- تتوقف "تعاريف" الجريمة السيبرانية، في المقام الأول، على الغرض من استخدام المصطلح
- فالجريمة السيبرانية الأساسية تتمثل في عدد محدود من الأعمال التي تمس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها
- الأعمال المنفّذة بواسطة الحواسيب والرامية إلى تحقيق مكاسب شخصية أو مالية أو إحداث أضرار، بما في ذلك أشكال الجرائم المتصلة بالهوية وبمحتوى الحواسيب، لا يمكن تطويعها بسهولة لتندرج ضمن تعاريف قانونية لمصطلح جامع
- يلزم تعريف الأعمال الأساسية التي تشكِّل جريمة سيبرانية، وإن كان "تعريف" الجريمة السيبرانية لا يتسم بنفس القدر من الأهمية فيما يخص الأغراض الأخرى، كتحديد نطاق صلاحيات الهيئات المختصة بالتحريات والتعاون الدولي، حيث يفضل التركيز على الأدلة الإلكترونية فيما يخص أي جريمة، بدلا من التركيز على تركيبة واسعة واصطناعية "للجريمة السيبرانية"

يجب أن تكون الدراسة الشاملة بشأن الجريمة السيبرانية واضحة فيما يتعلق بمجموعة الأفعال التي تم تضمينها في هذا المصطلح. فكلمة "جريمة سيبرانية" ذاتها غير قابلة للتعريف الأحادي، وعلى الأرجح من الأفضل اعتبارها مجموعة من الأفعال أو السلوك بدلا من اعتبارها فعلا منفردا. ومع ذلك، فإنه يمكن وصف المضمون الأساسي للجريمة السيبرانية، على الأقل لأغراض هذه الدراسة. ويمكن تباعا تقسيم هذه الأفعال إلى فئات على أساس الركن المادي للجريمة وأسلوب ارتكابها.

مصطلح "الجريمة السيبرانية"

لقد حاولت عدة أعمال أكاديمية تعريف "الجريمة السيبرانية"،[2] وفي هذا الصدد، لم يبدِ التشريع الوطني اهتماما إزاء وجود تعريف دقيق للكلمة. وفي مستعرض رد الدول على الاستبيان الملحق بهذه الدراسة، وُجد أن

[1] الاستبيان الخاص بدراسة الجريمة السيبرانية، السؤال رقم 81.

[2] Among various others, International Telecommunication Union, 2011. *Understanding Cybercrime: A Guide for Developing Countries*; Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185; Pocar, F., 2004. New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research,* 10(1):27-37; Wall, D.S., 2007. *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

عددا من الدول أشارت إلى ما يقرب من 200 مادة من مواد التشريع الوطني، فأقل من 5 في المائة استعملت كلمة "جريمة سيبرانية" في عنوان التشريع أو في نطاق الأحكام التشريعية[1]. ومن المسميات الأكثر شيوعا، إلى حد ما، في التشريعات؛ "*جرائم الحاسوب*"،[2] "*الاتصالات الإلكترونية*"،[3] "*تكنولوجيا المعلومات*"،[4] أو "*جرائم التكنولوجيا المتقدمة*".[5] فمن الناحية العملية، قننت العديد من هذه التشريعات جرائم جنائية والتي تم تضمنيها في مفهوم الجريمة السيبرانية، مثل النفاذ غير المشروع إلى نظام حاسوبي، أو التدخُّل في النظم الحاسوبية أو البيانات الحاسوبية. فإذا استخدم التشريع مصطلح "جريمة سيبرانية" بشكل محدّد في عنوان أحد القوانين أو الفصول (مثل: "قانون الجريمة السيبرانية") فنادرا ما يشتمل الفصل التعريفي في التشريع على تعريف لكلمة "جريمة سيبرانية".[6] وعندما تم إدراج مصطلح "جريمة سيبرانية" كتعريف قانوني، فالنهج الشائع قد دأب على تعريفها بـ "*الجرائم المشار إليها في هذا القانون*".[7]

وبطريقة مماثلة، فإن عددا قليلا من الصكوك الدولية أو الإقليمية تضمنت تعريفا للجريمة السيبرانية. فعلى سبيل المثال: خلت كل من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذلك مشروع اتفاقية الاتحاد الأفريقي، من تعريف الجريمة السيبرانية لأغراض الاتفاقية. بالإضافة إلى ذلك؛ لم تستخدم اتفاقية دول الكومنولث المستقلة حول التعاون في مكافحة الجرائم في مجال المعلومات الحاسوبية مصطلح "جريمة سيبرانية"،[8] ولكنها عرفتها باعتبارها "جريمة تتعلق بالمعلومات الحاسوبية": "*فعل إجرامي يستهدف المعلومات الحاسوبية*".[9] وعلى النهج نفسه؛ تضمنت اتفاقية منظمة شنغهاي للتعاون تعريف "المعلومات الحاسوبية" بأنها "*استخدام موارد المعلومات و (أو) التأثير عليها في المجال المعلوماتي لأغراض غير مشروعة*".[10]

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 12.

[2] أُنظر على سبيل المثال: قانون جرائم الحاسوب الماليزي 1997، قانون جرائم الحاسوب السيرلنكي 2007، قانون جرائم الحاسوب السوداني 2007.

[3] See, for example, Albania, Electronic Communications in the Republic of Albania, Law no. 9918 2008; France, Code des postes et des communications électroniques (version consolidée) 2012; Tonga, Communications Act 2000

[4] See, for example, India, The Information Technology Act 2000; Saudi Arabia, IT Criminal Act 2007; Bolivarian Republic of Venezuela, Ley Especial contra los Delitos Informáticos 2001; Vietnam, Law on Information Technology 2007

[5] See, for example, Serbia, Law on Organization and Competence of Government Authorities for Combating High-Tech Crime 2010.

[6] أُنظر على سبيل المثال: بوتسوانا، قانون جرائم الإنترنت والحاسوب 2007، بلغاريا؛ الفصل التاسع، القانون الجنائي رقم 92 لسنة 2002، كمبوديا مشروع قانون جرائم الإنترنت 2012، جامايكا، قانون الجرائم المتعلقة بالشبكات الإلكترونية 2010، ناميبيا، قانون إساءة استعمال الحاسوب والجرائم الحاسوبية 2003؛ السنغال، القانون رقم 2008-11 المتعلقة بجرائم الإنترنت 2008

[7] أُنظر على سبيل المثال: عمان، مرسوم ملكي رقم 12 لسنة 2011 بإصدار قانون مكافحة جرائم الإنترنت، الفلبين، قانون مكافحة الجرائم الإلكترونية 2012.

[8] The original agreement is in Russian language and uses the term 'преступление в сфере компьютерной информации', rather than the contemporary equivalent to 'cybercrime': 'киберпреступности

[9] الاتفاقية المتعلقة بالتعاون بين بلدان كومنولث الدول المستقلة، الفقرة (أ) المادة الأولى.

[10] اتفاق منظمة شنغهاي، الملحق (1).

هذا، وتُظهر النُهج التعريفية المستقرة في الصكوك الوطنية والدولية والإقليمية الطريقة التي عوّلت عليها هذه الدراسة، فالأخيرة لا تسعى "لتعريف" الجريمة السيبرانية في حد ذاتها، بل بالأحرى، تحدد قائمة، أو(سَلّة) من الأفعال التي يمكن أن تشكل جريمة سيبرانية، ويصاحب ذلك ميزة وضع التركيز على وصف دقيق للسلوك الذي ينبغي تجريمه. وعلى هذا النحو؛ فمن الأفضل عدم اعتبار كلمة "جريمة سيبرانية" مصطلحا قانونيا قائما بذاته.[1] ومن الجدير بالذكر في هذا المقام، أن هذا يعادل النهج الذي اعتمدته الصكوك الدولية، مثل اتفاقية الأمم المتحدة لمكافحة الفساد.[2] فهذه الاتفاقية لا تعرّف "الفساد"، ولكن بالأحرى تلزم الدول الأعضاء بتجريم مجموعة محددة من السلوك الذي يمكن وصفه على نحو أكثر فعالية.[3] ولذلك؛ من الأفضل اعتبار "الجريمة السيبرانية" بمثابة مجموعة من الأفعال أو السلوك.

وصف المفاهيم المحيطة

ومن الأمور المفيدة في هذا الصدد، تناول مواصفات المفاهيم المحيطة بالجريمة السيبرانية، مثل "الحاسوب"، "نظام الحاسوب"، "البيانات" و"المعلومات". وتعتبر دلالة هذه المفاهيم أمرا جوهريا لفهم الأشياء و/أو المصالح القانونية التي تحظى بالحماية، والتي تعتبر محل الجريمة السيبرانية. ويُظهر استعراض الصكوك الدولية والإقليمية نهجين رئيسيين: (1) مصطلح قائِم على بيانات أو نظام "الحاسوب"، (2) مصطلح مُسْتَنِد إلى بيانات أو نظام "المعلومات".[4] غير أن، تحليل عناصر التعاريف يشير إلى أن المصطلحات يمكن اعتبارها قابلة للتبديل إلى حد كبير. ويوضح الشكل التالي عناصر مشتركة من هذه التعريفات، فعلى الرغم من اختلاف المسميات إلا أن عددا من المفاهيم الأساسية تعتبر متجانسة.

---

[1] أُنظر أيضا: الاتحاد الدولي للاتصالات 2011: *Understanding Cybercrime: A guide for Developing Countries*

[2] أُنظر أيضا: اتفاقية الأمم المتحدة لمكافحة الفساد 2004.

[3] المرجع السابق، المادة 15وما يليها.

[4] تستخدم اتفاقية مجلس أوروبا بشأن جرائم الحاسوب وقانون الكومنولث النموذجي بشأن الجريمة السيبرانية مصطلحات "نظم الحاسوب" و"بيانات الحاسوب". ويستخدم ومشروع اتفاقية الاتحاد الأفريقي مصطلح "نظام الحاسوب" و"البيانات الحاسوبية". أما قرار الاتحاد الأوروبي حول الهجمات ضد نظم المعلومات يستخدم "نظم المعلومات" و"بيانات الحاسوب". أما اتفاقية الدول العربية تستخدم مصطلح "نظم وبيانات المعلومات". وأخيرا، تستعمل اتفاقية الكومنولث للدول المستقلة مصطلح "معلومات الحاسوب".

نظم الحاسوب/المعلومات

- جهاز [أو أجهزة مترابطة] والتي [تستند إلى برنامج حاسوب/معلومات] يؤدي [[تلقائي] معالجة بيانات/معلومات الحاسوب] [وظائف منطقية/حسابية/تخزين] [بما في ذلك بيانات/معلومات الحاسوب تخزين/معالجة/استرجاع/نقل من قِبَل نظام الحاسوب/معلومات] [بما في ذلك، أي وسيلة اتصالات أو معدات] [بما في ذلك شبكة الإنترنت].

برنامج الحاسوب/المعلومات

- تعليمات [في شكل مقروءة آليا] والتي [تمكن نظام الحاسوب/المعلومات] لكي [تقوم بمعالجة بيانات/معلومات الحاسوب] [أداء وظيفة/عمل] [يمكن تنفيذها من قِبَل نظام الحاسوب/المعلومات].

بيانات الحاسوب/المعلومات

- تقديم وقائع/معلومات/مفاهيم [في شكل مقروءة آليا] [مناسبة للمعالجة برنامج حاسوب/معلومات] [أو نظام حاسوب/معلومات] [بما في ذلك برنامج حاسوب/معلومات]

وتتجسد السمة الأساسية للمواصفات القانونية "لنظام الحاسوب" أو "نظام المعلومات"، على سبيل المثال، في وجوب "قدرة" الجهاز على معالجة بيانات الحاسوب أو المعلومات.[1] وتشير بعض المقاربات إلى أنه يجب أن تكون عملية المعالجة "تلقائية" أو "ذات سرعة عالية" أو "تبعا لبرنامج".[2] بيد أن بعض الاتجاهات تمدد من نطاق التعريف بالأجهزة التي تقوم بعملية تخزين أو إرسال أو استقبال معلومات أو بيانات حاسوبية،[3] في حين ذهبت بعض الاتجاهات الأخرى إلى إدراج تعريف البيانات الحاسوبية التي قام النظام بمعالجتها ضمن التعريف بالأجهزة.[4] فإذا كان مصطلح "نظام الحاسوب" أو "نظم المعلومات" يستبعد البيانات المخزّنة في النظام أو في أجهزة التخزين الأخرى من نطاق التعريف، فغالبا ما يتم تناولها بشكل منفصل في الأحكام القانونية

[1] أنظر على سبيل المثال: اتفاقية مجلس أوروبا بشأن جرائم الحاسوب، المادة 1.

[2] أنظر على سبيل المثال: مشروع الميثاق النموذجي لدول الكوميسا المادة 1، نصوص القانون النموذجي للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 3.

[3] مشروع اتفاقية الاتحاد الأفريقي، الجزء الثالث، الفصل الأول، فقرة6/1 من المادة الثالثة.

[4] قرار دول الاتحاد الأوروبي بشأن الهجمات ضد أنظمة المعلومات، فقرة (أ) من المادة الأولى.

الموضوعية الواردة في الصك.[1] بينما تعرّف بعض الصكوك كلا من "الحاسوب" و"نظام الحاسوب"، فإن الأخير يشتمل عادة على الأول، إلا أن سياق استخدام كلا المصطلحين في الصك يشير إلى عدم وجود فارق له دلالة من الناحية العملية،[2] غير أن الصكوك الأخرى – في هذا الصدد – تعنى بتعريف كل من "الحاسوب" و"نظام الحاسوب".[3] ونؤكد مرة أخرى على أنه يمكن أن يشتمل الأخير على الأول، ولا يوجد فرق مُغَايِر في استخدامهما داخل الصك ذاته.

تعتبر الصكوك القانونية الدولية والإقليمية بشأن مكافحة الجريمة السيبرانية "محايدة تكنولوجيا" بالدرجة الأولى في نصوصها، حيث لا تتضمن بشكل محدّد قائمة بالأجهزة التي قد تُعتبر من قبيل نظم الحاسوب أو نظم المعلومات. ففي معظم السياقات يعتبر هذا النهج من قبيل الممارسات الجيدة بِقَدْرِ ما تحدّ من مخاطر التكنولوجيات الجديدة التي تقع خارج نطاق الأحكام القانونية، حيث تدعو الحاجة إلى تحديث مستمر للتشريع.[4] فمن المرجح، تأسيسا على المفهوم الجوهري لمعالجة البيانات أو المعلومات الحاسوبية، أن تطبّق الأحكام تطبيقا نموذجيا على الأجهزة مثل خوادم الحاسوب وأجهزة الحاسوب التقليدية، كما تسري أيضا على أجهزة الحاسوب المكتبية الشخصية، وأجهزة الحاسوب المحمولة، والهواتف الذكية، والأجهزة اللوحية، بالإضافة إلى وسائل النقل والآلات المزوّدة بحواسيب على متنها، وكذلك أجهزة الوسائط المتعددة مثل الطابعات، ومشغلات الـ MP3، والكاميرات الرقمية، وماكينات المقامرة.[5] وهناك اعتقاد راسخ في إطار مفهوم "معالجة البيانات الحاسوبية والمعلومات" بأن أي جهاز، مثل أجهزة التوجيه اللاسلكي أو الثابتة، والتي تتصل بالإنترنت يعتبر أيضا من الأجهزة التي تسري عليها الأحكام. فقد تكون، على وجه التحديد، وسائط تخزين معلومات مثل الأقراص الصلبة أو ذاكرة الناقل التسلسلي العالمي (USB) أو بطاقات العرض السريع، جزءا من "نظام الحاسوب" أو "نظام المعلومات"، أو قد تكون غير ذلك. ولكن إذا خرجت من نطاق "نظام الحاسوب" أو "نظام المعلومات"، فإنها يمكن أن تظل أشياء ذات صلة من خلال أحكام قانونية منفصلة.

ويشير واحد فقط من الصكوك الدولية أو الإقليمية إلى أن مصطلح "تكنولوجيا غير متطورة" يقتصر فقط على وصف نظام الحاسوب، حيث اقتضى أن المصطلح لا يشتمل على: "آلة كاتبة آلية، أو طابعة

[1] أنظر أيضا على سبيل المثال: اتفاقية مجلس أوروبا بشأن جرائم الحاسوب، المادة 19، الصلاحيات الإجرائية للسلطات المختصة بالبحث أو الوصول المماثل (أ) نظام حاسوب أو جزء منه، بالإضافة إلى البيانات المخزنة فيه، (ب) وسائط تخزين البيانات الحاسوبية (الذاكرة) التي يمكن أن تخزن هذه البيانات.

[2] مشروع الميثاق النموذجي لدول الكوميسا، الجزء الأول، فقرة (ب)، (هـ) من المادة 1.

[3] الاتفاقية العربية، فقرة 5، 6 من المادة الثانية.

[4] أنظر على سبيل المثال: التقرير التفسيري لاتفاقية مجلس أوروبا بشأن جرائم الحاسوب، سلسلة المعاهدات الأوروبية رقم 185.

[5] انتهت أحد المذكرات التوجيهية لاتفاقية مجلس أوروبا بشأن جرائم الحاسوب إلى نتيجة مفادها أن تعريف "نظام الحاسوب" الوارد في الفقرة (أ) من المادة الأولى من اتفاقية مجلس أوروبا بشأن جرائم الحاسوب يتناول الأنماط المتطورة من التكنولوجيا التي تتجاوز أجهزة الحاسوب التقليدية أو نظم الحاسوب المكتبي، مثل الهواتف المحمولة الحديثة والهواتف الذكية وأجهزة المساعد الرقمي الشخصي، الحاسوب اللوحي أو ما شابه ذلك. أنظر: مجلس أوروبا 2012، المذكرة التوجيهية لاتفاقية مجلس أوروبا بشأن جرائم الحاسوب رقم 1 بشأن مفهوم "ماهية نظام الحاسوب" (2012)، 21–14 تشرين الثاني/نوفمبر 2012.

ضوئية، أو آلة حاسبة صغيرة محمولة باليد، أو أي أجهزة أخرى مماثلة".[1] ومع اتجاه العالم نحو "الأشياء المتصلة بالإنترنت" وأجهزة الحاسوب متناهية الصغر، فإن مواصفات مثل "نظام الحاسوب" أو "نظام المعلومات"، سوف تحتاج على الأرجح إلى أن تفسر على أنها متضمنة لمجموعة أكبر من الأجهزة[2]. ومع ذلك، فإن المفهوم الأساسي لـ "المعالجة الآلية للمعلومات" من حيث المبدأ يبدو مرنا بما فيه الكفاية ليتضمن، على سبيل المثال، رصد ورقابة آلية ذكية تعمل بتقنية التواصل قريب المدى، وموصولية برتوكولات الإنترنت القائمة داخل الأجهزة المنزلية.

عادة ما توصف "البيانات الحاسوبية" أو "المعلومات الحاسوبية" بأنها *"تمثل معطيات أو معلومات أو مفاهيم يمكن أن يقوم الحاسوب بقراءتها أو معالجتها أو تخزينها"*. وتوضّح بعض الاتجاهات أن "البيانات الحاسوبية" أو "معلومات الحاسوب" تتضمن برامج الحاسوب،[3] في حين أن الآخرين غضوا النظر عن هذه النقطة. فالاختلاف بين طرائق "القراءة الآلية" و"القراءة أو المعالجة أو التخزين بواسطة نظام حاسوبي (أو معلومات حاسوبية)" تعتبر طبيعة دلالية فقط. فمن الناحية العملية، تشتمل بيانات الحاسوب أو المعلومات في الأغلب على بيانات أو معلومات مخزنة في وسائط تخزين مادية (مثل: الأقراص الصلبة، ذاكرة الناقل التسلسلي العالمي أو بطاقات العرض السريع)، حيث تُخزن البيانات أو المعلومات في نظام ذاكرة الحاسوب أو نظام المعلومات، كما تشتمل أيضا على عمليات إرسال البيانات أو المعلومات (سواء السلكية أو البصرية أو تردد راديوي)، ووحدات العرض المادي للبيانات أو المعلومات في شكل مطبوع أو على شاشة الجهاز، على سبيل المثال.

ومع الإقرار بالنهج المختلفة في استخدام المصطلح، فإن هذه الدراسة عند استخدامها لمصطلحي "نظام الحاسوب" و"البيانات الحاسوبية" فإنها تتعامل معهما بشكل مُتَكافِئ مع مصطلحي "نظام المعلومات" و"المعلومات الحاسوبية".

فئات الجريمة السيبرانية

يعتبر مصطلح "الجريمة السيبرانية" من المصطلحات غير القابلة لمدلول أحادي، إلا أن ثمة سؤال يطرح حول إن كان من الممكن تحديد أهداف أو سمات أو أسلوب الجريمة السيبرانية، بدلا من (أو بالإضافة إلى) تحديدها استنادا إلى قائمة من أفعال فردية من الجريمة السيبرانية. وعلى النحو المذكور أعلاه، فإن مثالا على هذا النهج يمكن أن نجده في اتفاقية دول الكومنولث المستقلة، حيث تصف *"الجريمة المتعلقة بالمعلومات الحاسوبية"*

---

[1] مشروع القانون النموذجي لدول الكوميسا، الجزء الأول، فقرة (ب) مادة 1.

[2] في إطار استعراض التطورات المحتملة والتحديات التنظيمية المرتبطة بالأشياء المتصلة بالإنترنت، أنظر الاتحاد الأوروبي 2009. الاتصالات من المفوضية إلى البرلمان الأوروبي، والمجلس، واللجنة الاقتصادية والاجتماعية الأوروبية، ولجنة الأقاليم. الأشياء المتصلة بالإنترنت–خطة عمل لـ *Europe*. COM (2009) 278 Final، 18 حزيران/يونيو 2009.

[3] اتفاقية مجلس أوروبا بشأن جرائم الحاسوب، فقرة (ب)، مادة 1.

بأنها *"فعل إجرامي هدفه المعلومات الحاسوبية."* [1] بينما تصف اتفاقية منظمة شنغهاي للتعاون (على نطاق أوسع) *"جرائم المعلومات"* بأنها *"استخدام موارد المعلومات و (أو) التأثير عليها في الفضاء المعلوماتي لأهداف غير مشروعة."* أما اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية – وعلى الرغم من عدم تعريفها للمصطلحات – فإنها تستخدم عناوين تجريم واسعة، تشتمل على *"جرائم ضد سِرية، وسلامة، وتوافر البيانات والأنظمة الحاسوبية"*، و*"جرائم ذات صلة بالحاسوب"*، و*"جرائم ذات صلة بالمحتوى"*.[2] أما مشروع قانون الاتحاد الأفريقي، فيستخدم على نحو مشابه عناوين تجريم تميّز بين *"جرائم خاصة بتكنولوجيات المعلومات والاتصال"* و*"جرائم ذات تكييف قانوني محلها تكنولوجيات المعلومات والاتصال"*.[3]

ويتضح من هذه النُهُج أن هناك عددا من السمات العامة يمكن استعمالها لوصف أفعال الجريمة السيبرانية. فإحدى هذه النُهُج تركز على *الهدف* المادي للجريمة – فهل الهدف يتمثل في الشخص، أو الشيء، أو في قيمة المستهدف من الجريمة.[4] وقد ظهر هذا النهج في اتفاق كومنولث الدول المستقلة (حيث هدف الجريمة معلومات حاسوبية)، وكذلك في العنوان الأول الأساسي للفصل الأول المعني بالقانون الجنائي لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية (حيث أهداف الجريمة بيانات حاسوبية أو نظم الحاسوب). وتبنى نهج آخر فكرة مفادها ما إذا كانت نظم الحاسوب أو نظم المعلومات تشكل جزءا لا يتجزأ من أسلوب ارتكاب الجريمة[5]. وظهر أيضا هذا النهج في العنوان الأساسي الثاني والثالث والرابع للفصل الأول المعني بالقانون الجنائي لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، وكذلك في اتفاقية منظمة شنغهاي للتعاون، وفي مشروع اتفاقية الاتحاد الأفريقي. وهكذا فإن تحديد الأهداف المحتملة للجريمة السيبرانية وأسلوب ارتكابها لا يصف أعمال الجريمة السيبرانية برمتها، وإنما يمكن أن يقدم بشكل عام عددا من التصنيفات المفيدة التي قد يتم تصنيف أفعال ضمنها بشكل عام.

وفي الواقع، تتبنى بعض الصكوك الدولية والإقليمية المعنية بالجريمة السيبرانية مفهوما ضيقا للأنظمة أو البيانات الحاسوبية لتكون محل الجريمة.[6] في حين أن الصكوك الأخرى تتناول نطاقا عريضا من الجرائم، تتضمن أفعالا حيث يكون محل الجريمة شخصا أو شيئا ما ذو قيمة، أو بالأحرى نظام حاسوبي أو بيانات حاسوبية، ولكن أينما يعتبر نظام حاسوبي أو نظام معلومات – مع ذلك – جزءا لا يتجزأ من أسلوب ارتكاب الجريمة.[7]

---

[1] اتفاقية كومنولث الدول المستقلة، فقرة (أ) مادة 1.

[2] اتفاقية مجلس أوروبا بشأن جرائم الحاسوب، العناوين 1، 2، و3.

[3] مشروع اتفاقية الاتحاد الأوروبي، الجزء الثالث، الفصل الخامس، الجزء الثاني، الفصل الأول والثاني.

[4] تلك التي تشكل جرائم ضد السرية، النزاهة، وتوافر البيانات ونظم الحاسوب. أنظر على سبيل المثال:

Calderoni, F., 2010. The European legal framework on cybercrime: striving for an effective implementation. *Crime, Law, and Social Change,* 54(5):339-357

[5] Podgor, E.S., 2002. International computer fraud: A paradigm for limiting national jurisdiction. *U.C. Davis Law Review*, 35(2):267- 317, 273 et seq

[6] قرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات، اتفاقية كومنولث للدول المستقلة.

[7] For instance, ECOWAS Draft Directive, Art. 17 (Facilitation of access of minors to child pornography, documents, sound or pornographic representation). See also Pocar, F., 2004. New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research*, 10(1):27-37.

ويتناول الفصل الرابع (التجريم) أفعالا محددة جرّمتها هذه الصكوك على نحو مفصل. وبينما لا تستعمل كل الصكوك الدولية أو الإقليمية مفهوما واسعا لماهية الجريمة السيبرانية، إلا أن النهج المأخوذ من هذه الدراسة يهدف إلى أن يكون المفهوم شاملا بقدر المستطاع. ولذلك؛ تستعمل الدراسة قائمة عريضة لمواصفات الأفعال التي تشكل الجريمة السيبرانية، حيث قامت الدراسة بتصنيفها بصفة عامة ضمن ثلاث فئات على أساس محل الجريمة وأسلوب ارتكابها. ونظرا لاستخدام طريقتين للتصنيف، فقد يوجد قدر ما من التداخل بين الفئات الثلاث.

الأفعال التي تشكل الجريمة السيبرانية

يطرح الشكل التالي 14 فعلا من الأفعال التي قد تشكل الجريمة السيبرانية، وتم تقسيم هذه الأفعال إلى ثلاث فئات عريضة، ويقدم المرفق الأول بهذه الدراسة وصفا تفصيليا أكثر لكل فعل من هذه الأفعال. كما تم أيضا استخدام هذه القائمة من الأفعال في الاستبيان المرسل إلى الدول، وكيانات القطاع الخاص، والمنظمات الحكومية الدولية، وكذلك المؤسسات الأكاديمية، وذلك لجمع معلومات ذات صلة بهذه الدراسة.[1] وتهدف هذه القائمة إلى تقديم مجموعة أولية من الأفعال التي يمكن إدراجها تحت مصطلح "الجريمة السيبرانية"، بهدف إرساء أساس تحليلي خلال الدراسة. كما أنه ليس مقصودا من القائمة أن تكون شاملة، مع الأخذ في الاعتبار أن المصطلحات المستخدمة والمصاحبة للمواصفات في المرفق الأول لا ترمي إلى تقديم تعريفات قانونية، بل تعتبر

أفعال ضد سرية، ونزاهة، وتوافر البيانات أو النظم الحاسوبية

- النفاذ غير المشروع إلى نظام حاسوبي
- النفاذ إلى، أو الاعتراض، أو الحصول غير المشروع على بيانات حاسوبية
- التدخل غير المشروع مع نظام أو بيانات حاسوبية
- إنتاج، أو توزيع أو حيازة أدوات لإساءة استعمال الحاسوب
- إنتهاك تدابير حماية الخصوصية أو البيانات

أفعال متعلقة بالحاسوب تهدف إلى كسب شخصي أو مالي أو إضرار

- الاحتيال أو التزوير المتعلق بالحاسوب
- جرائم الهوية المتعلقة بالحاسوب
- جرائم حقوق الطباعة والعلامة التجارية المتعلقة بالحاسوب
- إرسال أو التحكم في إرسال البريد الإلكتروني الطفيلي
- الأفعال المسببة لأذى شخصي والمتعلقة بالحاسوب
- إغواء أو استمالة الأطفال لأغراض جنسية من خلال الحاسوب

أفعال متعلقة بمحتوى الحاسوب

- الأفعال المرتكبة بواسطة الحاسوب والمنطوية على خطاب كراهية
- إنتاج أو توزيع أو حيازة مواد إباحية متعلقة بالأطفال بواسطة الحاسوب
- أعمال دعم جرائم الإرهاب بواسطة الحاسوب

---

[1] قد تم أَسَاسا وَفِي الْبِدَايَة تطوير مشروع الاستبيان الخاص بهذه الدراسة المعنية بجمع المعلومات من قبل الأمانة العامة استنادا إلى قائمة بموضوعات بغية إدراجها في الدراسة، والتي وافق عليها فريق الخبراء المعني بالجريمة السيبرانية (الواردة في تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية (E/CN.15/2011/19)). تم إرسال مشروع الاستبيان، بما في ذلك المشروع الأول من مواصفات فعل الجريمة السيبرانية، لجميع البلدان للتعليق في عام 2011. وعقب إدْراج الأمانة العامة التعليقات الواردة، فقد تم الموافقة على الاستبيان النهائي بما فيه قائمة الأفعال المذكورة هنا، وتمت الموافقة من قبل مكتب فريق الخبراء المعني بالجريمة السيبرانية في جلسته المنعقدة في 19كانون الثاني/ يناير 2012

هذه المصطلحات بمثابة "مواصفات إجمالية للفعل" والتي قد استخدمت كنقطة انطلاق للتحليل والمناقشة. وجدير بالذكر أن هذه الدراسة لم "تعرّف" الجريمة السيبرانية (سواء مع تعريف مرافق للمصطلح ذاته، أو عن طريق قائمة "قَطْعِيّة" للأفعال)، بيد أن السلوك المدرج – مع ذلك – قد يعتبر المحتوى الأساسي لمعنى المصطلح، على الأقل لأغراض هذه الدراسة.[1]

وتجدر الإشارة هنا إلى أنه في هذه المرحلة وفي ظل الوجود المطلق للإنترنت وأجهزة الحاسوب الشخصي، فإن ذلك يعني أن النظم أو البيانات الحاسوبية تعتبر عاملا مُسَاعِدا – على الأقل في الدول المتقدمة – في أي جريمة جنائية تقريبا. ولذلك؛ ترتبط الجريمة السيبرانية ارتباطا وثيقا بمجال الأدلة الإلكترونية، إلا أن ذلك يختلف من الناحية النظرية. حيث يُعتبر جمع الأدلة الإلكترونية وتقديمها جزءا لا يتجزأ من عمليات التحقيق والملاحقة القضائية للجريمة السيبرانية. وهذا الحال أيضا في الجرائم التقليدية على نحو متزايد، مثل جرائم السرقة والنهب، أو السطو المسلح، فضلا عن أشكال الجريمة المنظمة أيضا. فقد تحتوي سجلات الهاتف المحوسبة، ورسائل البريد الإلكتروني، وسجلات الاتصال ببرتوكولات الإنترنت، وخدمة الرسائل القصيرة، وسجلات العناوين في الهاتف المحمول، وملفات الحاسوب، على أدلة تشير على مكان الجريمة أو الدافع للجريمة، أو وُجُود مسرح الجريمة، أو المساهمة الجنائية للمشتبه فيه في أي شكل من أشكال الجريمة.

أفعال التعدّي على سرية وسلامة وتوافر البيانات أوالنظم الحاسوبية

تستهدف القائمة الأساسية للأفعال التي تشكل الجريمة السيبرانية نظام الحاسوب أو البيانات الحاسوبية. وتشتمل الخطوات الأساسية على النفاذ غير المشروع إلى نظام حاسوبي، أو بيانات حاسوبية، أو اعتراض هذه البيانات، أو الاطِّلاع عليها. يتناول الفصل الرابع (التجريم) هذه الأفعال بدرجة كبيرة، سواء على عينة من القوانين الوطنية وعينة من الصكوك الدولية والإقليمية. فمثل هذه الأفعال يمكن ارتكابها بوسائل عديدة مختلفة، فعلى سبيل المثال النفاذ غير المشروع لنظام حاسوبي قد يتكون من استخدام غير مصرح به لكلمة مرور تم الكشف عنها، أو الوصول عن بعد باستخدام برمجيات مميزة.[2] وقد تشكل هذه البرمجيات أيضا تدخلا في البيانات الحاسوبية و/أو النظام الحاسوبي. ومن ثم، يمكن أن تظهر الأفعال الفردية درجة من التداخل عبر جريمة من الجرائم "قائمة". وتتضمن الفئة الأولى أيضا أفعالا تتعلق بالأدوات التي يمكن استخدامها لتنفيذ

---

[1] في إطار الرد على التعليقات الواردة من الدول، فقد تم إجراء تعديلات على قائمة الأفعال الواردة في هذا الفصل، بالمقارنة مع تلك المستخدمة في الاستبيان الخاص بهذه الدراسة. وقد حملت الفئة الثانية في الاستبيان الخاص بهذه الدراسة عنوان "الأفعال ذات الصلة بالحاسوب بهدف تحقيق مكاسب شخصية أو مالية". ولقد تم تعديل هذا العنوان ليكون "الأفعال ذات الصلة بالحاسوب بهدف تحقيق مكاسب شخصية أو مالية أو إلحاق الضرر". أما الفئة الثالثة من الاستبيان الخاص بهذه الدراسة كان تحت عنوان "الأفعال المحددة ذات الصلة بالحاسوب". ولقد تم تعديل هذا العنوان ليكون "الأفعال ذات الصلة بمحتوى الحاسوب". وتم ترحيل البندين: "الأفعال ذات الصلة بالحاسوب التي تسبب في إلحاق ضرر شخصي" و"الأفعال ذات الصلة بالحاسوب بغرض إغواء أو استمالة الأطفال لأغراض جنسية من الفئة الثالثة إلى الفئة الثانية. بالإضافة إلى ذلك، تتضمن الاستبيان الخاص بهذه الدراسة البند التالي: "الأفعال ذات الصلة بالحاسوب وتنطوي على عنصرية أو كراهية الأجانب. ولقد تم تعديل هذا البند أيضا وتمديد نطاقه ليشمل "الأفعال ذات الصلة بالحاسوب وتنطوي على خطاب كراهية".

[2] الأمم المتحدة 1994، دليل الأمم المتحدة بشأن منع ومكافحة الجريمة المتعلقة باستخدام الحاسوب.

أعمال ضد نظم الحاسوب أو بياناته.[1] وأخيرا، تشتمل الفئة على أعمال إجرامية تتعلق بسوء التعامل مع البيانات الحاسوبية طبقا لمتطلبات محددة.

> **"عملية أورورا"**
>
> في عام 2010، قامت العديد من شركات البرمجيات رفيعة المستوى بالإبلاغ عن سلسلة من الهجمات عبر الإنترنت، وفي النهاية قد سُجلت إختراقات في محرك بحث لشركة كبيرة. وباستخدام نقطة ضعف في أحد متصفّحات شبكة الإنترنت، قام المهاجمون بعمل نفق داخل شبكة داخلية عبر حواسيب عمل الموظفين المعرضة للخطر، وتمكنوا من الدخول على حسابات البريد الإلكتروني واختراق مركز تخزين شفرة المصدر المؤَمّنة عَلَى نَحْوٍ غَيْرِ مُلائِم.
>
> وفي نفس العام، تلقى مستخدمو موقع تواصل إجتماعي رسائل بريد إلكترونية من حساب وهمي مع روابط لنظام تسجيل دخول زائف ليبدو أنه مرسل من الشركة، وبالفعل قام المستخدمون الضحايا بالدخول والتسجيل. وأصبحت وثائق المستخدمين عرضة للخطر، ومن المحتمل أن يصبح المضيف المخترق أحد الأعضاء في شبكة البوت نت "ZeuS".
>
> المصدر: Trustwave. 2011. SpiderLabs Global Security Report

الأفعال المتصلة بالحواسيب التي تُرتكب لتحقيق مكسب أو ضرر شخصي أو مالي

تركز الفئة الثانية على الأفعال التي يعتبر فيها النظام الحاسوبي بمثابة الأسلوب الأساسي المستخدم في ارتكاب الجريمة، ويصاحب ذلك اختلاف في محل هذه الأفعال الإجرامية. ففي حالة الاحتيال باستخدام الحاسوب، تعتبر المقتنيات الاقتصادية محل الجريمة. أما في حالة جرائم حقوق المؤلف والعلامات التجارية المرتكبة بواسطة الحواسيب، فإن محل الجريمة يتمثل في حقوق الملكية الفكرية المحمية، أما في حالة الأعمال المرتكبة بواسطة الحواسيب والتي تتسبّب بضرر شخصي، مثل استخدام نظام حاسوبي في المضايقة، أو التسلط، أو التهديد، أو التعقب، أو التسبب في خوف أو ترهيب للفرد، أو "استمالة" طفل ما، ومن ثم؛ فمحل هذه الجريمة يعتبر الفرد.

> **فيروس "GOZI"**
>
> في أوائل عام 2013، اتهمت النيابة العامة في أمريكا الشمالية ثلاثة رجال أوروبيين بإنتاج وتوزيع فيروس حاسوبي ألحق الضرر بأكثر من مليون جهاز حاسوب على مستوى العالم، وتمكنوا من الوصول إلى معلومات بشأن حسابات بنكية شخصية، واستولوا على 50 مليون دولار أمريكي على الأقل في الفترة ما بين 2005 إلى 2011. فهذا الفيروس قد تم انتاجه في أوروبا ثم انتشر في أمريكا الشمالية، حيث ألحق الضرر بأجهزة حاسوب تخص هيئات وطنية. وتجرى حاليا إجراءات تسليم اثنين من المتهمين. وقد وصفت هذه القضية بأنها: *"واحدة من أكثر عمليات الدمار المالي التي لم نشاهد مثلها حتى الآن"*.
>
> المصدر: http://www.fbi.gov/

إن العمل التمهيدي بشأن وضع إطار لتصنيف دولي للجرائم لأغراض إحصائية، يدعم الرأي القائل بأن مجموعة متنوعة من الأعمال بأهداف إجرامية مادية مختلفة يمكن بالرغم من ذلك اعتبارها "جريمة سيبرانية". يشير العمل الذي اضطلع به مؤتمر الإحصائيين الأوروبيين إلى أن الأفعال التي تشكل "جريمة سيبرانية" يمكن تسجيلها، لأغراض إحصائية، باستخدام "وسم العلامة"، والتي من شأنها أن تعبّر عن تيسير

[1] Examples include Low orbit ion cannon (LOIC), sKyWIper and the ZeuS banking malware

استخدام الحاسوب لفعل محدد داخل (كامل) نظام تصنيف الجريمة. ومثل هذه "العلامة" يمكن تطبيقها، من حيث المبدأ، على الأعمال التي ييسرها الحاسوب والتي تقع في أي مكان ضمن نظام أكبر لتصنيف الجريمة، وما إذا كانت هذه الأعمال ضد شخص، أو أعمال ضد الملكية، أو أعمال ضد النظام العام أو السلطة.[1]

يتمثل أحد التحديات المتعلقة باستخدام الحاسوب في ارتكاب جرائم سيبرانية في امتداد فئة المخاطر لتشمل بطريقة أخرى مجموعة كبيرة من جرائم ترتكب دون الاتصال بالإنترنت، من خلال استخدام أو مساعدة نظام حاسوبي. ويثور تساؤل ما إذا كان هذا النوع من الجريمة يجب اعتباره من قبيل "الجريمة السيبرانية"، أم يزال الأمر مطلقا. وبينما تتضمن بعض الصكوك الدولية والإقليمية عددا محدودا وقليلا نسبيا من الجرائم ذات الصلة بالحاسوب، إلا أن الصكوك الأخرى توسعت في هذا الصدد. فعلى سبيل المثال؛ تتناول اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية (من هذه الفئة) جرائم التزوير والاحتيال باستخدام الحاسوب مُنْفَرِدة.[2] وعلى النقيض من ذلك، فإن القانون العربي النموذجي يتضمن أحكاما جنائية بشأن استعمال الحاسوب في التزوير، والتهديد، والابتزاز، والاستيلاء على ممتلكات منقولة، أو سند قانوني من خلال استخدام احتيالي لأحد الأسماء، أو الحصول بشكل غير مشروع على أرقام أو تفاصيل بطاقة الائتمان، أو التربح بصورة غير مشروعة من خدمات الاتصالات، أو إنشاء صفحة ويب بهدف الاتجار في البشر أو المخدرات أو المؤثرات العقلية، وكذلك استخدام الحاسوب في تحويل الأموال غير المشروعة أو التَسَتّر على مصدرها غير المشروع.[3]

وعلى عكس تلك الأفعال التي نوقشت سابقا، هناك عمل آخر يمكن إدراجه ضمن هذه الفئة. ويتمثل حصريا في إرسال رسائل البريد الإلكتروني الطفيلي أو التحكم بإرسالها.[4] وبينما إرسال رسائل البريد الإلكتروني الطفيلي غير المرغوب فيها أمر محظور من قبل جميع مقدمي خدمة الإنترنت، إلا أن هذا الأمر لم يجرّم عالميا من جانب الدول. ويُلقي الفصل الرابع (التجريم) الضوء على هذه المسألة بمزيد من التفصيل.

الأفعال ذات الصلة بالمحتوى الحاسوبي

أما الفئة الأخيرة من أفعال الجريمة السيبرانية فتتمثل في تلك المتعلقة بالمحتوى الحاسوبي؛ وتتمثل في الكلمات والصور والأصوات، والصور المرسلة أو المخزنة من قبل نظم حاسوبية، بما في ذلك الإنترنت. حيث يعتبر الهدف المادي للعمل الإجرامي في الجرائم المتعلقة بالمحتوى في أغلب الأحيان هو شخص ما، أو جماعة محددة من الأشخاص أو شيء ما ذا قيمة كبيرة، أو عَقِيدَة ما. وبنفس النهج كما في الفئة الثانية، يمكن من حيث المبدأ أن تُرتكب هذه الأفعال بدون الاتصال بالإنترنت، فضلا عن استخدم نظم حاسوبية في ذلك. ومع ذلك، تُعَيّن العديد من الصكوك الدولية والإقليمية المعنية بمكافحة الجريمة السيبرانية أحكاما بشأن المحتوى

---

[1] أنظر: لجنة الأمم المتحدة الاقتصادية لأوروبا، مؤتمر الإحصائيين الأوروبيين. مبادئ وإطار تصنيف دولي للجرائم لأغراض إحصائية. ECE/CES/BUR/2011/NOV/8/Add.1، 11تشرين الثاني/نوفمبر 2011

[2] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادتان 7 و8.

[3] القانون العربي النموذجي، المواد 4 و9-12 و17-19

[4] يشير إرسال أو التحكم بإرسال الرسائل غير المرغوب فيها إلى الأعمال التي تنطوي على استخدام نظام حاسوبي لإرسال رسائل إلى عدد كبير من المستقبلين بدون طلب أو إذن. أنظر الملحق الأول (مواصفات الفعل الاجرامي)

الحاسوبي.[1] بيد أن هناك رأيا أحاديا يطالب بإدراج الأفعال المتعلقة بالمحتوى الحاسوبي ضمن مصطلح "الجريمة السيبرانية"، ويعلل ذلك، بأن النظم الحاسوبية، بما في ذلك الإنترنت، قد غيرت بشكل جذري نطاق ومدى نشر المعلومات.[2]

قد تعتبر بعض الدول أن حيازة مجموعة من المحتويات الصريحة أو نشرها عبر نظم حاسوبية بمثابة سلوك إجرامي. ومن المهم في هذا الصدد ملاحظة أن نقطة الانطلاق الرئيسية في المعاهدات الدولية المعنية بحقوق الإنسان تتجسد في حرية الرأي والتعبير،[3] مع الأخذ في الاعتبار مبدأ سيادة الدولة. ومن هذا المنطلق؛ يجيز القانون الدولي فرض بعض القيود الضرورية على النحو المنصوص عليه في القانون.[4] علاوة على ذلك، فإن القانون الدولي يلزم الدول بحظر الأنماط المستخدمة في التعبير، بما في ذلك استغلال الأطفال في المواد الإباحية، والتحريض المباشر والعلني على ارتكاب جريمة الإبادة الجماعية، وأشكال الخطابات التي تنطوي على كراهية، والتحريض على الإرهاب.[5] ويتناول الفصل الرابع (التجريم) النهج الدولية والإقليمية لتجريم الأفعال المتعلقة بالمحتوى الحاسوبي، بما في ذلك من وجهة نظر القانون الدولي لحقوق الإنسان، على نحو مفصل.

مؤامرة للتحضير لعمل إرهابي

في أيار/مايو من عام 2012، قضت إحدى المحاكم بغرب أوروبا بحبس أحد مواطنيها خمس سنوات للمشاركة في مؤامرة جنائية بهدف التخطيط للقيام بعمل إرهابي. وقدم ممثل الادعاء العام للمحكمة العشرات من رسائل البريد الإلكتروني التي تم فك شفرتها تتضمن محتويات ذات نزعة جهادية، والتي قد أُرسلت من بين أمور أخرى إلى الموقع الإلكتروني لرئيس البلاد، منسوبة إلى عضو في جماعة متطرفة تعمل على الصعيد العالمي. وأصدرت المحكمة أمر تحفّظ مكّن السلطات من تحديد التواصل بين عضو الجماعة المتطرفة ومواقع إلكترونية لجماعات متطرفة، بما في ذلك، موقع إلكتروني هدفه استضافة ونشر وثائق، وتسجيلات صوتية ومرئية، وبيانات من أمراء حرب ومهاجمين انتحاريين، ومواد تخص جماعات متطرفة أخرى. ويشير هذا إلى أن المتهم قام بشكل نشط، في جملة أمور، بعمليات ترجمة وتشفير وضغط ملفات، وتخليق كلمات مرور لحماية مواد مؤيدة لاتجاهات جهادية، والتي قام لاحقا بعد ذلك بتحميلها وتعميمها عبر شبكة الإنترنت، علاوة على ذلك؛ اتخاذ خطوات ملموسة لتوفير الدعم المالي للجماعة المتطرفة، بما في ذلك محاولة لاستخدام "باي بال" (PayPal) وغيرها من أنظمة الدفع الافتراضية. وتوافرت لدى المحكمة الأدلة الكافية المطلوبة لإثبات أن المتهم لم يقدم فقط الدعم الفكري، بل قام أيضا قدم الدعم اللوجستي المباشر لخطة إرهابية محددة وواضحة المعالم.

المصدر: مكتب الأمم المتحدة المعني بالمخدرات والجريمة. 2012. استعمال الإنترنت لأهداف إرهابية.

[1] أنظر: المادة (9) من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والمادة (12) وما يليها من اتفاقية جامعة الدول العربية لمكافحة جرائم تقنية المعلومات، وأُنظر كذلك: نصوص القانون النموذجي للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، الجزء الثاني، من بين أمور أخرى.

[2] Marcus, R.L., 2008. The impact of computers on the legal profession: Evolution or revolution? *Northwestern University Law Review,* 102(4):1827-1868

[3] المادة 19 من الإعلان العالمي لحقوق الإنسان، المادة 19 من العهد الدولي الخاص بالحقوق السياسية والاقتصادية، المادة 9 من الاتفاقية الأوروبية بشأن حماية حقوق الإنسان والحريات الأساسية، المادة 13 من الاتفاقية الأمريكية لحقوق الإنسان، المادة 9 من الميثاق الأفريقي لحقوق الإنسان والشعوب.

[4] Cassese, A., 2005. *International Law.* 2nd ed. Oxford: Oxford University Press. p.53. and pp.59 et seq.

[5] الجمعية العامة للأمم المتحدة 2011، تعزيز وحماية الحق في حرية الرأي والتعبير، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي A/66/290، 10آب/ أغسطس 2011.

وقد أُدرجت أعمال دعم جرائم الإرهاب باستخدام الحاسوب ضمن فئة الجريمة السيبرانية ذات الصلة بالمحتوى الحاسوبي. ويُظهر المنشور الذي صدر مؤخرا عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بعنوان "استخدام الإنترنت لأغراض إرهابية"،[1] أن النظم الحاسوبية قد تُستعمل في مجموعة من الأعمال التي من شأنها أن تعزز الإرهاب وتدعمه. وتشتمل هذه الأعمال على الدعاية (بما في ذلك التجنيد، والتطرف والتحريض على الإرهاب)، والتمويل، والتدريب، والتخطيط (بما في ذلك من خلال الاتصالات السرية والمعلومات المستقاة من مصادر مفتوحة) والتنفيذ، والهجمات السيبرانية.[2] الاستبيان المستخدم لجمع المعلومات لهذه الدراسة أشار مباشرة إلى جرائم التحريض على الإرهاب، وتمويل الإرهاب التي تتم من خلال الحاسوب، والتخطيط لجرائم إرهابية.[3] وبذلك فإن هذه الدراسة تعنى فقط بمجالات المحتوى الحاسوبي المتعلقة بجرائم الإرهاب، وتستثني تهديد الهجمات السيبرانية من قبل منظمات إرهابية من مجال التحليل — وهذا النهج يعادل نهج منشور مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن استخدام الإنترنت لأغراض إرهابية.

أفعال جريمة سيبرانية أخرى

لا تعد القائمة التي ضمت 14 فعلا من أفعال الجريمة السيبرانية شاملة، ويتضح ذلك من خلال جمع المعلومات لأغراض هذه الدراسة، حيث تمت دعوة الدول لتحديد الأفعال الأخرى التي تراها أيضا تشكل الجريمة السيبرانية.[4] وتضمنت الردود ما يلي: *"استخدام الحاسوب لتسهيل الأعمال غير المشروعة المرتبطة بالصكوك المالية ووسائل الدفع"* ، و*"المقامرة عبر الإنترنت"* ، و*"استخدام إحدى وسائل تقنية المعلومات لأغراض الاتجار بالبشر"* ، و*"استخدام الحاسوب في الأعمال المرتبطة بالاتجار في المخدرات"* ، و*"استخدام الحاسوب في الأعمال المرتبطة بالحصول على المال بطريقة ابتزازية أو من خلال التهديد"* ، و*"الاتجار بكلمات المرور"* ، و*"الدخول إلى معلومات سرية"* .[5] ففي هذه الحالات، ذكرت الردود أن التشريعات السيبرانية المحددة قد تناولت هذه الأفعال، مما يؤكد استخدام النظم الحاسوبية أو البيانات الحاسوبية في الفعل الذي يشكل الجريمة السيبرانية.

في بعض هذه الحالات، يمكن النظر للفعل على اعتباره أحد الأشكال المتخصصة أو إحدى الأفعال المختلفة للجريمة السيبرانية المدرجة بالفعل. فعلى سبيل المثال، قد يكون استخدام أو حيازة أدوات ذات صلة بالحاسوب لارتكاب جرائم مالية، مشمولا بفعل شامل من أعمال الاحتيال أو التزوير ذات الصلة بالحاسوب.[6] وقد يعتبر الوصول إلى معلومات سرية بمثابة مجموعة فرعية من الوصول غير المشروع إلى البيانات الحاسوبية بصفة

---

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة 2012، استخدام الإنترنت في لأغراض الإرهابية، متوفر على الرابط التالي:
https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[2] الاستبيان الخاص بدراسة الجرائم السيبرانية. قسم مواصفات الفعل الإجرامي. أنظر أيضا الملحق الأول (مواصفات الفعل الإجرامي).

[3] الاستبيان الخاص بدراسة الجرائم السيبرانية. قسم مواصفات الفعل الإجرامي. أنظر أيضا الملحق الأول (مواصفات الفعل الإجرامي).

[4] الاستبيان الخاص بالدراسة، السؤال رقم 39.

[5] المرجع السابق.

[6] بعض الدول على سبيل المثال، تدرج الفعل الخاص بحيازة أجْهِزَ ة للاستخدام في عمليات الاحتيال ضمن جرائم الاحتيال الجنائية.

عامة. أما فيما يتعلق بالاتجار في كلمة المرور، فقد تناولتها بعض من الأحكام المعنية بسوء استخدام أدوات الحاسوب.[1]

تثير أعمال أخرى، مثل استخدام الحاسوب في الأعمال المرتبطة بالحصول على المال بطريقة ابتزازية أو من خلال التهديد،[2] تحديا يتمثل في إدراج (أو عدم إدراج) الجرائم المرتكبة دون الاتصال بالإنترنت، والتي قد انتقلت بدرجات متفاوتة مباشرة على الإنترنت، وتم مناقشة هذه النقطة بإيجاز في سياق الأعمال ذات الصلة بالحاسوب لتحقيق مكاسب شخصية أو مالية أو إلحاق الضرر بالآخرين. وكما لاحظ عدد من البلدان المجيبة على الاستبيان الخاص بهذه الدراسة، أن المبدأ العام المتكرر يتمثل في "ما هو غير قانوني دون الاتصال بالإنترنت يعتبر أيضا غير قانوني عبر الاتصال بالإنترنت".[3] وفي العديد من الحالات، يمكن أيضا تطبيق القوانين الجنائية المعنية بتنظيم السلوك دون الاتصال بالإنترنت على النسخ الإلكترونية على شبكة الإنترنت لنفس السلوك. ولذلك، قد قامت العديد من الدول، على سبيل المثال، بتفسير القوانين التقليدية المعمول بها لتتناول استخدام الحاسوب في الجرائم المرتبطة بالحصول على المال بطريقة ابتزازية أو من خلال التهديد،[4] أو استخدام نظم الحاسوب لتسهيل

الإنترنت وبيع المخدرات غير المشروعة

منذ منتصف عام 1990، بدأ الاستخدام المتزايد للإنترنت من قبل تجار المخدرات لبيع المخدرات غير المشروعة، أو لبيع السلائف الكيمائية المطلوبة لتصنيع هذه المخدرات. وفي الوقت نفسه، تُعلِن الصيدليات غير المشروعة على الإنترنت عن مبيعات غير مشروعة في شكل وصفات طبية لعامة الناس، بما في ذلك المواد الخاضعة للمراقبة الدولية. فمن المستقر أن هذه المواد تخضع لثلاث معاهدات دولية لمراقبة المخدرات، وتشمل مسكّنات شبه أفيونية، منشطات الجهاز العصبي المركزي، المهدئات والمؤثرات العقلية الأخرى. فالعديد من الأدوية المعروضة للبيع بهذه الطريقة إما قد تحولت من سوق مشروع، أو قد تحولت إلى سوق غير مشروع لبيع أدوية مُقلّدة أو مغشوشة تشكل خطرا على صحة المستهلكين. وفي هذا الصدد، هناك حقيقة واقعية مؤداها أن العديد من الصيدليات غير المشروعة على الإنترنت تجري عملياتها من جميع مناطق العالم، ولديها القدرة على نقل أعمالها بسهولة عند الإغلاق النهائي لأحد المواقع التابعة لها، مما يعني ذلك ضرورة اتخاذ إجراءات فعالة في هذا المجال.

وفي عام 2009، نشرت الهيئة الدولية لمراقبة المخدرات "المبادئ التوجيهية للحكومات بشأن منع بيع المواد غير المشروعة الخاضعة للرقابة الدولية عبر الإنترنت". تتناول هذه المبادئ التوجيهية أهمية تخويل السلطات المختصة صلاحية التحقيق واتخاذ الإجراءات القانونية ضد الصيدليات غير المشروعة على الإنترنت والمواقع الأخرى التي تُستعمل للبيع غير المشروع للمواد المراقبة دوليا، وكذلك حظر شحنها عن طريق البريد مع ضمان إعتراض هذه الشحنات، علاوة على ذلك، وضع معايير للممارسة المهنية الجيدة لتوفير الخدمات الصيدلانية عن طريق الإنترنت.

[1] لم يتم تضمين الاتجار بكلمات السر للحاسوب، أو رموز الوصول، أو البيانات المماثلة صراحة في وصف الفعل الوارد في البند الخاص "بإنتاج أو توزيع أو حيازة أدوات إساءة استخدام الحاسوب" المستخدم في الاستبيان الخاص بالدراسة، مما دفع بعض الدول إلى تحديد هذا السلوك كعمل ملحق.

[2] بالإضافة إلى استخدام نظم الحاسوب في الابتزاز أو التهديد، فإن ذلك يمكن أن يرتبط بالتدخل غير المصرح به لأنظمة الحاسوب أو البيانات الحاسوبية، أو طلب المال المترابط بهجمات في شكل حجب الخدمة الموزعة.

[3] الاستبيان الخاص بالدراسة، السؤال رقم 39.

[4] أنظر على سبيل المثال:
Landgericht Düsseldorf, Germany. 3 KLs 1/11, 22 March 2011, in which the accused was convicted of extortion and computer sabotage against online betting sites through the hired services of a botnet.

عمليات الاتجار في البشر.[1] وقد تناول الفصل الرابع (التجريم) بمزيد من التفصيل إحدى الممارسات القانونية الوطنية في هذا الشأن.

وقد يبدو أن هناك نهجا وحيدا يدرج في وصف "الجريمة السيبرانية" فقط تلك الأعمال التي اعتبرت استخدام نظام الحاسوب جزءا لا يتجزأ من نطاق التغير الجذري للفعل المرتكب دون الاتصال بالإنترنت أو طبيعته، بطريقة أخرى.[2] ويعتبر تحديد الاتجاه هنا من الأمور البالغة الصعوبة، إلا أنه من المناسب القول – على سبيل المثال – بأن استخدام النظم الحاسوبية يعتبر من الأمور التي تغير قواعد اللعبة أساسا، ولكن متى يتعلق الأمر بطبيعة ونطاق جريمة الاحتيال على المستهلك ولكن ليس بهدف الاتجار في العقاقير المخدرة؟ وهل استخدام الخدمات المالية عبر الإنترنت لإخفاء الربح الأصلي المتأتي من ارتكاب جريمة[3] يختلف بشكل كبير عن المعاملات المالية التقليدية مما يستلزم تحديد استخدام الحاسوب في غسل الأموال كجريمة منفصلة. وتمثل قائمة الـ 14 فعلا الواردة في هذه الدراسة، إلى حد ما، محاولة لاستنباط الممارسات المعاصرة بشأن تلك الأفعال التي تعتبر بصفة عامة "جريمة سيبرانية".

وتجدر الإشارة إلى أن الأعمال الأخرى التي تشكل الجريمة السيبرانية التي أشارت إليها بعض الدول، ولاسيما المقامرة عبر الإنترنت، قد لا تجرّم باستمرار في دول أخرى، فالمقامرة عبر الإنترنت مسموح بها في العديد من الدول، ولكنها محظورة بشكل مباشر أو غير مباشر في دول أخرى.[4] بغض النظر عن الوضع القانوني للمقامرة عبر الإنترنت، فإن مواقع المقامرة قد تكون في كثير من الأحيان هدفا للاحتيال الحاسوبي أو اعتراض البيانات الحاسوبية أو التدخل غير المشروع.[5] وقد يجرى أحيانا تمييز في سياق المصطلح العام "المقامرة عبر الإنترنت"بين شبكة الإنترنت باعتبارها مجرد وسيلة اتصال؛ مثل المقامرة عبر شبكة اتصالات عن بعد كما يحدث في العالم المادي، وبين نادي القمار الافتراضي حيث لا يملك المقامر وسيلة للتحقق من نتائج اللعبة.[6]

[1] مبادرة الأمم المتحدة العالمية لمكافحة الاتجار بالبشر 2008، ومنتدى فيينا لمكافحة الاتجار بالبشر ورقة معلومات أساسية لـ 17 ورشة عمل تحت عنوان: التكنولوجيا والاتجار بالبشر. متاح على الرابط التالي:
http://www.unodc.org/documents/human-trafficking/2008/BP017TechnologyandHumanTrafficking.pdf
وتشمل قاعدة بيانات مكتب الأمم المتحدة المعني بالمخدرات والجريمة المعنية بالاتجار بالبشر؛ عددا من قضايا تنطوي على استخدام الإنترنت لنشر إعلانات https://www.unodc.org/cld/index.jspx للمزيد من المعلومات، أنظر أيضا الرابط التالي:
https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html?ref=menuside

[2] قد يمكن تطبيقها، على سبيل المثال، في سياق جرائم الاعتداء الجنسي على الأطفال، عندما يقوم الجاني بعمل الصور دون الاتصال بالإنترنت ثم يشارك، في وقت لاحق، عبر الإنترنت شبكات من أفراد يحملون نفس التفكير، فالأعمال الإضافية لتوزيع واستلام وجمع المادة محل الفعل غير المشروع "عبر الإنترنت" تعتبر جريمة جنائية جديدة. يمكن الحصول على لمحة عامة عن هذا الأسلوب ومزيد من الأمثلة من خلال: وزارة الداخلية البريطانية 2010، استراتيجية الجريمة السيبرانية، صفحة 45.

[3] لجنة الخبراء التابعة للمجلس الأوروبي المعنية بتقييم تدابير مكافحة غسل الأموال وتمويل الإرهاب 2012. تدفق المال الإجرامي عبر الإنترنت: الطرق والاتجاهات وإحباط محاولات أصحاب المصالح المتعددين.

[4] Fidelie, L.W., 2008. Internet Gambling: Innocent Activity or Cybercrime? *International Journal of Cyber Criminology*, 3(1):476-491; Yee Fen, H., 2011. Online Gaming: The State of Play in Singapore. *Singapore Academy of Law Journal*, 23:74.

[5] أنظر على سبيل المثال: McMullan, J.L., Rege, A., 2010. Online Crime and Internet Gambling. *Journal of Gambling Issues*, 24:54-85.

[6] Pereira de Sena, P., 2008. Internet Gambling Prohibition in Hong Kong: Law and Policy. *Hong Kong Law Journal*, 38(2):453-492.

وفي أغلب الأحيان يميّز بين نوادي القمار الافتراضية والمقامرة دون الاتصال بالإنترنت، ويرجع ذلك إلى إمكاناتها للمشاركة القسرية والاحتيال[1] وسوء الاستخدام من قبل القُصّر. ووفقا لمبدأ السيادة الوطنية، فقد أدرك أحد النهج الإقليمية، على الأقل، حق الدول في وضع أهداف سياستها بشأن الرهان والمقامرة طبقا لنطاق قيمها وتحديد التدابير التقييدية المناسبة.[2] ولذلك، قد يواجه إدراج المقامرة عبر الإنترنت في وصف عام للجريمة السيبرنية تحديات بشأن عالمية تجريمه.

استعراض

من الجدير بالذكر، أن الدول المجيبة لم تحدد نطاقا واسعا للسلوك خارج الأفعال التي تشكل الجريمة السيبرانية والتي حددتها بـ 14 عملا تم إدراجه في الاستبيان الخاص بالدراسة. ولذلك قد توجد بعض درجات التوافق بشأن جوهر السلوك، على الأقل، المدرج في مصطلح "الجريمة السيبرانية".

على الرغم من ذلك، وكما تمت مناقشته في هذه الدراسة، فإن مسألة تحديد إذا ما كان من الضروري إدراج سلوك معين في وصف "الجريمة السيبرانية" يعتمد إلى حد كبير على الغرض من استخدام مصطلح "جريمة سيبرانية" في المقام الأول.

وفقا للمنظور القانوني الدولي، فإن مضمون المصطلح يعتبر بوضوح ذا صلة عندما يتعلق الأمر باتفاقيات للتعاون الدولي. تتجسد إحدى سمات الصكوك الدولية والإقليمية بشأن الجريمة السيبرانية، على سبيل المثال، في وجود سلطات تحقيق متخصصة، وهذا ما تفتقر له الصكوك التي تخلو من أعمال سيبرانية محددة.[3] وافقت الدول الأعضاء في الصكوك على توفير هذه الصلاحيات للدول الأطراف الأخرى من خلال طلبات المساعدة القانونية المتبادلة. في حين أن لدى بعض الصكوك نطاقا عريضا من الصلاحيات تمكّن من جمع الأدلة الإلكترونية لأي جريمة جنائية،[4] إلا أن بعض الصكوك الأخرى تحدّ من نطاق التعاون الدولي وصلاحيات التحقيق في "الجريمة السيبرانية"، أو "الجرائم المتصلة بالمعلومات الحاسوبية"،[5] إن مفاهيم "الجريمة السيبرانية" في إطار المجال الدولي قد يكون لديها آثار تتمثل في توافر سلطات التحقيق والوصول إلى أدلة إلكترونية تتخطى الحدود الإقليمية. ويتناول الفصل السابع (التعاون الدولي) هذه المسألة بمزيد من التفصيل.

---

[1] أنظر على سبيل المثال: محكمة العدل الأوروبية شركة ***Sporting Exchange Ltd*** ضد الوزير ***van Justitie*** في القضية رقم C-203/08 الفقرة 34: " نظرا لعدم وجود اتصال مباشر بين المستهلك والمشغل، فإن ألعاب الحظ يمكن الوصول إليها عبر الإنترنت حيث تنطوي على مخاطر مختلفة وكبيرة من الاحتيال من قبل المشغلين بالمقارنة مع الأسواق التقليدية لمثل هذه الألعاب".

[2] المرجع السابق، الفقرة 28.

[3] تتضمن مثل هذه الصلاحيات، إصدار أوامر بشأن البيانات الحاسوبية المخزنة، وتحديد الوقت الحقيقي لجمع البيانات الحاسوبية، وكذلك إصدار أوامر عاجلة بالتحفظ على البيانات الحاسوبية. أنظر على سبيل المثال: مشروع اتفاق الاتحاد الأفريقي، مشروع القانون النموذجي لدول الكومسا، القانون النموذجي لدول الكومنولث، اتفاقية مجلس أوروبا بشأن الجرائم السيبرانية، واتفاقية جامعة الدول العربية.

[4] أنظر على سبيل المثال: اتفاقية مجلس أوروبا بشأن الجرائم السيبرانية، واتفاقية جامعة الدول العربية.

[5] أنظر على سبيل المثال: الاتفاق المتعلق بالتعاون بين الدول الأعضاء في كومنولث الدول المستقلة لمكافحة الجرائم في مجال المعلومات الحاسوبية، ومشروع اتفاق الاتحاد الأفريقي

وبينما يتحرك العالم نحو الوصول إلى الإنترنت عالميا، فإن مفاهيم الجريمة السيبرانية ستحتاج إلى العمل على عدة مستويات: التحديد والتفصيل في حالة تعريف أعمال فردية محددة من أعمال الجريمة السيبرانية ولكنها واسعة بما فيه الكفاية لضمان أن سلطات التحقيق وآليات التعاون الدولي يمكن تطبيقها، مع ضمانات فعالة، على الانتقال المستمر للجرائم التي ترتكب بدون الاتصال بالإنترنت إلى متغيرات عبر الإنترنت.

الفصل الثاني: الصورة العالمية

بَعْد لمحة موجزة عن النهج المستخدمة لقياس الجريمة السيبرانية، فإن هذا الفصل يرسم صورة للجريمة السيبرانية على الصعيد العالمي لمن "هو" المنخرط في الجريمة السيبرانية (وكم عددهم)، و"ماهية" الأفعال التي تشكلها (وكم قدرها). فقد وجد أن أفعال الجريمة السيبرانية وزعت على نطاق واسع عبر الفئات المختلفة للجريمة السيبرانية، مع ارتفاع معدلات ضحايا الجريمة السيبرانية عن ضحايا الجريمة التقليدية في كثير من الحالات. وبينما تعتمد سمات الجناة على نوع الفعل السيبراني، فإن التقديرات تشير إلى أنَّ مصدر أكثر من 80 في المائة من الجريمة السيبرانية هو شكل من أشكال النشاط المنظم.

1-2 قياس الجريمة السيبرانية

الاستنتاجات الرئيسية:

- تتضمن مصادر المعلومات لقياس الجريمة السيبرانية إحصاءات الجرائم المسجّلة لدى الشرطة: (والاستقصائيات الخاصة بالسكان والمنشآت التجارية والمبادرات الخاصة ببلاغات الضحايا والمعلومات الخاصة بالأمن السيبراني القائم على التكنولوجيا
- من المستبعد أن تكون الإحصاءات التي طالبت بقياس الجريمة السيبرانية باعتبارها ظاهرة شاملة قابلة للمقارنة بالجرائم المرتكبة عبر الحدود الوطنية. توفر البيانات المصنفة طبقا لفعل الجريمة السيبرانية المباشر درجة عالية من الاتساق والتَجانُس
- بينما تعتبر إحصاءات الجرائم المسجّلة لدى الشرطة ذات قيمة لمنع الجريمة على المستوى الوطني وصناعة السياسات، إلا أنها لا تتناسب بصفة عامة لإجراء مقارنات مع الجريمة السيبرانية المرتكبة عبر الحدود الوطنية. ويمكن أن تقدم البيانات المستمدة من الاسْتِقْصاء ومصدر المعلومات القائمة على التكنولوجيا مَدَارِك قيمة
- مصدر المعلومات المستخدم في هذه الدراسة للإجابة عن الأسئلة المتعلقة بـ من "هو" المنخرط في الجريمة السيبرانية (وكم عددهم)، و"*ماهية*" الأفعال التي تشكلها و"*كم قدرها*"

لماذا قياس الجريمة السيبرانية؟

نصّت المادة 11 من مبادئ الأمم المتحدة التوجيهية لمنع الجريمة[1] بضرورة أن تستند الاستراتيجيات والسياسات والبرامج والتدابير المتعلقة بمنع الجريمة إلى *"أساس عريض متعدد التخصصات من المعرفة بمشاكل الجريمة"* . يجب أن تتضمن هذه "القاعدة المعرفية" إنشاء "نظم البيانات".[2] ويعتبر جمع البيانات لإعداد إجراءات التدخُّل لمنع الجريمة والحد منها عملية لا تقل أهمية عن الجريمة السيبرانية كما هو الحال بالنسبة لأنواع الجرائم الأخرى. ويتبلور استخدام قياس الجريمة السيبرانية للإعلام عن مبادرات الحد من الجريمة؛ في: تعزيز الاستجابات المحلية والوطنية والإقليمية والدولية، وتحديد الفجوات في الاستجابات، وتوفير معلومات استخباراتية وتقييم للمخاطر، وتثقيف وتوعية الجمهور.[3]

يسلط العديد من المعلقين الضوء على التحديات الخاصة التي تعترض سبيل جمع المعلومات بشأن مَجَال وطبيعة الجريمة السيبرانية،[4] وتشتمل هذه التحديات على: إشكالية تحديد ما يُشكل الجريمة السيبرانية في المقام الأول؛ والتحديات المتعلقة بالنقص في التقارير المقدمة وتسجيل أعداد تقل عن العدد الحقيقي؛ واستعراض القضايا المنهجية والوعي؛ واحتمال حدوث تضارب في المصالح للبيانات الخاصة بالقطاع الخاص.[5]

أيّ جرائم يجب قياسها؟

لقد تناول الفصل السابق مسألة إمكانية إدراج الأعمال ذات الصلة بالمحتوى الحاسوبي ضمن مصطلح "الجريمة السيبرانية". ولأغراض القياس، فمن المرجح أن تكون الأفعال الواردة في الفئة الأولى من فئات الجريمة السيبرانية (أفعال ضد السرية، النزاهة، توافر بيانات حاسوبية أو نظم حاسوبية) والفئة الثالثة (الأفعال المتعلقة بالمحتوى الحاسوبي) مُحَدّدة بوضوح نسبيا. ومع ذلك، فإن مخاطر الأفعال الواردة في الفئة الثانية (بشأن استخدام الحاسوب في تحقيق مكاسب شخصية أو مالية، أو إلحاق الضرر بالآخرين) باتَت بالِغة. وفي ضوء ما تمت مناقشته من قبل؛ ما هو الحد الأقصى لإدراج نظم الحاسوب أو البيانات الحاسوبية، التي تجيز تسجيل جريمة ما باعتبارها جريمة سيبرانية، في هذه الفئة؟ وللإجابة على هذا السؤال؛ فإن المقاربات قد تختلف في هذه الصدد ولاسيما إذا تعلق الأمر بجرائم مسجلة لدى الشرطة. ويتناول الجزء التالي بمزيد من التفصيل إحصاءات الشرطة بشأن هذه المواجهة.

---

[1] المبادئ التوجيهية لمنع الجريمة، المرافقة لقرار المجلس الاقتصادي والاجتماعي للأمم المتحدة رقم 2002/13 بشأن إجراءات تعزيز مكافحة الجريمة، 24 تموز/يوليو 2002.

[2] المرجع السابق، فقرة (و) المادة 21.

[3] Fafinski, S., Dutton, W.H. and Margetts, H., 2010. *Mapping and Measuring Cybercrime.* Oxford Internet Institute Forum DiscussionPaper No. 18., June 2010

[4] See, for example, Brenner, S.W., 2004. Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology*, 9(13):1-52.Cybercrime is also included as an example of an 'emerging and difficult to measure crime' in documents of the 42nd Session of the United Nations Statistical Commission. See United Nations Economic and Social Council, Statistical Commission, 2012. *Report of the National Institute of Statistics and Geography of Mexico on Crime Statistics*. E/CN.3/2012/3, 6 December 2011

[5] Fafinski, S., Dutton, W.H. and Margetts, H., 2010. *Mapping and Measuring Cybercrime.* Oxford Internet Institute Forum Discussion Paper No. 18. June 2010

إنه من البَيِّن بشكل عُمُومِيّ أن الإحصاءات التي ترمي إلى قياس "الجريمة السيبرانية" باعتبارها ظاهرة منفردة تعتبر غير قابلة للمقارنة مع الجرائم المرتكبة عبر الحدود الوطنية، ويرجع ذلك إلى التباين الكبير في مضمون المصطلح بين نظم تسجيل الجرائم. ومن ثم، فالنهج المفضل في هذا الصدد يتمثل في النظام الذي يوفر بيانات مصنفة حسب فعل الجريمة السيبرانية المنفصل. فمثل هذا النهج يوفر درجة عالية من الاتساق والقابلية للمقارنة، ويتماشى علاوة على ذلك مع الممارسة الجيدة في مجال إحصاءات الجريمة والعدالة الجنائية بشكل عام.[1]

ماذا نريد أن نعرف؟

يهدف أحد النهج المعنية بقياس الأشكال والأبعاد الجديدة للجريمة، بما في ذلك الجريمة السيبرانية، إلى وَصَف من *"هو"* المنخرط في الجريمة السيبرانية (*وكم عددهم*)، و*"ماهية"* الأفعال التي تشكلها (*وكم قدرها*)[2]، وهذا يتطلَّب مجموعة *مؤتلفة* من مصادر البيانات، مثل المعلومات المتعلقة بالمرتكبين والمعلومات المتعلقة بالتدفُّقات داخل الأسواق غير المشروعة والمعلومات المتعلقة بأعداد الأحداث الإجرامية وما تسبِّبه من أضرار وخسائر وما ينتج عنها من تدفُّقات مالية غير مشروعة، حيث لدى كل عنصر من هذه العناصر آثار للتصدي للجريمة السيبرانية. وتعتبر هياكل وشبكات الجماعات الإجرامية المنظمة، على سبيل المثال، أمرا محوريا لتَخْطِيط التدخُّلات في مجال العدالة الجنائية. وجدير بالذكر، أن تفهما أفضل للأسواق غير المشروعة، مثل تركيز اقتصاد السوق السوداء على بيانات بطاقات الائتمان المسروقة، يقدم تفاصيل البواعث الكامنة للنشاط الإجرامي (بغض النظر عن الأفراد أو الجماعات المعنية)، وبالتالي؛ يعتبر ذلك بمثابة مداخل عدة لوضع برامج منع الجريمة. كما أن استيعاب حجم الأضرار والخسائر والمكاسب المالية غير المشروعة يقدم إرشادات بشأن إعطاء الأولوية للتدخلات.

أيّ المعلومات يمكن جمعها؟

توجد أربعة مصادر رئيسية للمعلومات لقياس *"ماهية"* الأفعال التي تشكل الجريمة السيبرانية وما مقدارها: (1) إحصاءات الجرائم المسجَّلة لدى الشرطة، (2) الاستبيانات الخاصة بالسكان والمنشآت التجارية، (3) المبادرات الخاصة ببلاغات الضحايا (4) المعلومات الخاصة بالأمن السيبراني القائم على التكنولوجيا. بالرغم من أن هذه القائمة ليست شاملة، إلا أنها تتناول المصادر الرئيسية للمعلومات والتي لديها قدر من المقارنة مع الجرائم المرتكبة عبر الحدود الوطنية. وثمة مصادر أخرى تشمل دراسات فردية بشأن الظواهر المحددة، مثل الزحف على عناوين الموارد الموحَّدة (URL crawling) وانتزاع السيطرة على شبكات الروبوت

---

[1] أنظر على سبيل المثال: تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة 2010، تحت عنوان "وضع معايير في مجال الإحصاءات القضائية والشؤون الداخلية– التشريعات الدولية وتشريعات الاتحاد الأوروبي"، وكذلك دليل الأمم المتحدة 2003 بشأن نظام إحصاءات العدالة الجنائية.

[2] European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), 2011. Data Collection on [New] Forms and Manifestations of Crime. *In:* Joutsen, M. (ed.) *New Types of Crime, Proceedings of the International Seminar held in Connection with HEUNI's Thirtieth Anniversary*, 20 October 2011, Helsinki: EICPC. See also UNODC, 2010. *The Globalization of Crime: A Transnational Organized Crime Threat Assessmen*

(botnettakeover).[1] ويتناول الملحق الثاني المرافق لهذه الدراسة نقاط القوة والتحديات المرتبطة بكل مصدر تباعا. ولقد وجد أنه في الوقت الحاضر، فإن إحصاءات الجريمة السيبرانية المسجلة من قبل بالشرطة ذات قيمة لمنع الجريمة وصناعة السياسات على الصعيد الوطني، لكنها لا تتناسب بصفة عامة لإجراء مقارنات في مجال الجريمة السيبرانية على الصعيد العابر للحدود. وعلى العكس من ذلك، فإن المعلومات القائمة على الاستبيان، ومعلومات الأمن السيبراني القائمة على التكنولوجيا، تقدم بعض الرؤى بشأن طبيعة ونطاق الظاهرة. وتستعمل مصادر المعلومات الواردة أدناه للتعامل مع الأسئلة حول "ماهية" و"مقدار" الجريمة السيبرانية. أما بخصوص السؤال المتعلق بـ "من" هم المتورطون في هذه الجرائم؛ فإن القسم التالي من هذا الفصل سيتناول مرتكبي الجريمة السيبرانية.

2-2 الصورة العالمية للجريمة السيبرانية

الاستنتاجات الرئيسية:

- تشمل الجريمة السيبرانية طائفة واسعة من الجرائم المرتكبة بدافع مالي والجرائم المتصلة بالمحتوى الحاسوبي، فضلا عن الأعمال التي تمس بسرية النظم الحاسوبية وسلامتها وقابلية النفاذ إليها
- تختلف تصوّرات الخطر والتهديد النسبيَّين بين الحكومات ومؤسسات القطاع الخاص
- تعتبر حالات التأذي الفردية من الجريمة السيبرانية أكثر بكثير من حالات التأذي من أشكال الجرائم "التقليدية". وتتراوح معدّلات التأذي من تزوير بطاقات الائتمان وانتحال الشخصية على الإنترنت والوقوع ضحية لمحاولات التصيُّد الاحتيالي ومحاولات الدخول دون إذن إلى حسابات البريد الإلكتروني بين 1 و17 في المائة من نسبة السكان
- معدلات حالات التأذي الفردية بسبب الجريمة السيبرانية أعلى في البلدان التي تشهد مستويات نمو منخفضة، مما يُبرز الحاجة إلى تعزيز جهود منع الجرائم في هذه البلدان
- أبلغت مؤسسات القطاع الخاص في أوروبا عن معدلات تأذي مماثلة – تراوحت بين 2 و16 في المائة – وكانت تتعلق بانتهاك البيانات بسبب الاقتحام أو التصيد الاحتيالي
- الساحة التي تُستخدَم فيها هذه الأدوات المختارة لارتكاب الجرائم، مثل "اعتداءات البوت نت"، هي ساحة عالمية. فقد كان أكثر من مليون عنوان فريد من عناوين بروتوكول الإنترنت يعمل على الصعيد العالمي كخادوم "بوت نت" للتحكُّم في شبكات الحواسيب ومراقبتها في عام 2011
- ومثّل محتوى الإنترنت أيضا مصدر قلق كبير للحكومات، فمن المواد المراد حذفها منه المواد الإباحية المتعلقة بالأطفال، والخطابات المفعمة بالكراهية، ومواد التشهير، وانتقاد الحكومات، الأمر الذي أثار شواغل متعلقة بقانون حقوق الإنسان في بعض الحالات

---

[1] أنظر على سبيل المثال:

Kanich, C. *et al.*, 2011. *No Plan Survives Contact: Experience with Cybercrime Measurement.* Available at: http://static.usenix.org/events/cset11/tech/final_files/Kanich.pdf ; see also Kemmerer, R.A., 2011. *How to Steal a Botnet and What Can Happen When You Do.* Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6080765

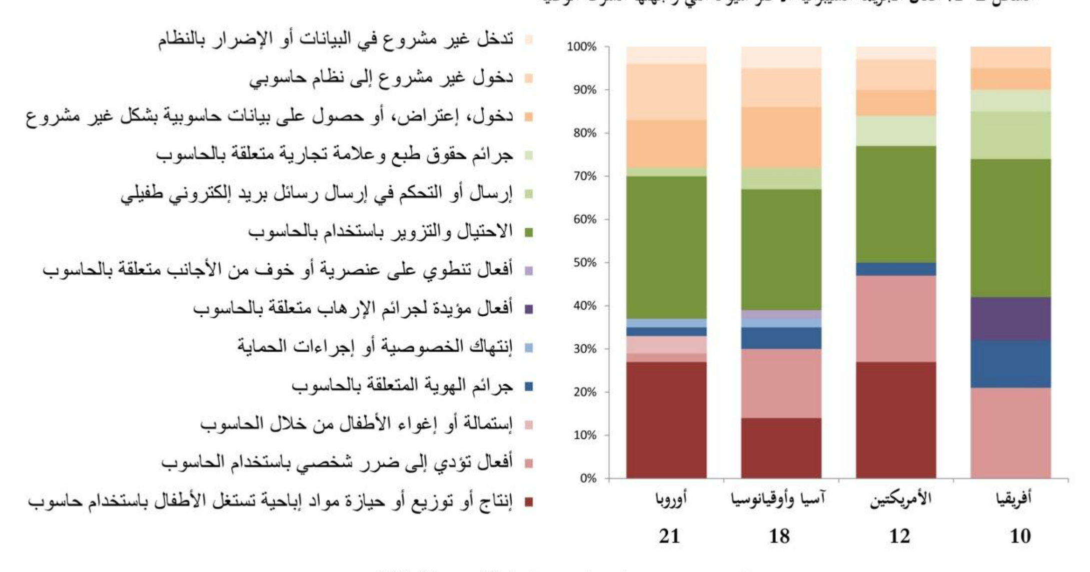
- يقدر أن حوالي 24 في المائة من إجمالي حركة الإنترنت العالمية تنتهك حقوق المؤلف

يرسم هذا الجزء صورة عالمية لطبيعة ونطاق الجريمة السيبرانية في ضوء البيانات التي تم الحصول عليها خلال جمع المعلومات، الخاصة بهذه الدراسة، من الدول والقطاع الخاص والمؤسسات الأكاديمية، فضلا عن مراجعة لأكثر من 500 مُؤَلّف عبر النشر المفتوح المصدر.[1]

توزيع أفعال الجريمة السيبرانية

تشمل الجريمة السيبرانية على طائفة واسعة من الجرائم. طبقا لملاحظات المؤسسات المكلفة بإنفاذ القانون، تشكل الأعمال المرتكبة بدافع مالي والجرائم المتصلة بالاحتيال والتزوير باستخدام الحاسوب ثلث الأعمال عَبْر جميع المناطق في جميع أنحاء العالم تقريبا. وقد ذكرت عدد من البلدان أن *"الاحتيال في التجارة الإلكترونية وعمليات الدفع"*، و*"الاحتيال على المواقع الإلكترونية المعنية بالمزادات مثل موقع إيباى (ebay)"*، و*"الاحتيال المتعلق بدفع الرسوم مقدما"*، و*"مخطَّطات الاحتيال عن طريق البريد الإلكتروني ومواقع التواصل الاجتماعي"*، من الأعمال التي كانت سائدة بشكل خاص. وكما هو مبين أدناه، يعتبر الأثر المالي لهذه الجريمة كبيرا.[2]

الشكل 2–1: أفعال الجريمة السيبرانية الأكثر شيوعا التي واجهتها الشرطة الوطنية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 80. (رقم=61، 140)

بيد أن في بعض المناطق هناك ما بين الثلث والنصف من أفعال الجريمة السيبرانية تتعلق *بالمحتوى* الحاسوبي، بما في ذلك المواد الإباحية التي تستغل الأطفال، والمحتوى المتصل بالجرائم الإرهابية، وكذلك تلك المتعلقة بانتهاك حقوق الملكية الفكرية. وقد تم تحديد الجرائم ذات الصلة بالمواد بالإباحية المتعلقة بالأطفال في

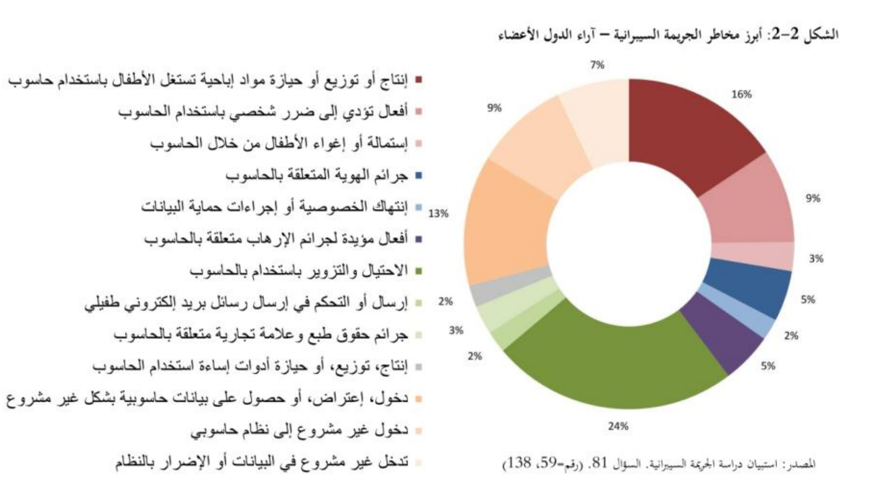
---

[1] المصادر بشأن هذا الملف متوفرة لدى الأمانة العامة للأمم المتحدة

[2] الاستبيان الخاص بالدراسة، السؤالين رقم 80، و85.

أوروبا والأمريكتين بشكل أكثر تواترا مما هو عليه الحال في آسيا وأوقيانوسيا أو أفريقيا، على الرغم من أن ذلك قد يتعلق بالاختلافات في تركيز هيئات إنفاذ القانون بين المناطق، أكثر منه بالاختلافات الأساسية. ومن ناحية أخرى؛ فقد تم تحديد الأعمال المرتكبة بواسطة الحواسيب والتي تتسبّب بضرر شخصي على نطاق واسع باعتبارها من الأعمال الأكثر شيوعا في أفريقيا والأمريكتين وآسيا وأوقيانوسيا مما هو سائد في هذا الصدد في أوروبا. ويتناول استعراض الأعمال ذات الصلة بالمحتوى الحاسوبي الإضافي أدناه مزيدا من هذه الاتجاهات.

وفقا لتصورات هيئات إنفاذ القانون، فإن الأفعال المرتكبة ضد السرية، والنزاهة، وتوافر بيانات حاسوبية أو نظم حاسوبية، مثل اقتحام نظام حاسوبي أو الاطِّلاع على بيانات حاسوبية بصورة غير مشروعة يشكل ما بين ثلث و10 في المائة من الأفعال، وهذا يعتمد على المنطقة التي ارتكب فيها الفعل. وتعتبر هذه الأفعال جزءا لا يتجزأ من الجريمة السيبرانية، فربما من ناحية تسهم قدرات الدول المختلفة في تحديد هذه الجرائم (أكثر تقنية) التي تؤثر في انتشارها الملموس عبر المناطق، وكذلك القدرات المختلفة على الملاحقة القضائية لمرتكبيها، ومن ناحية أخرى، كما تم تناوله أدناه، تظهر استبيانات

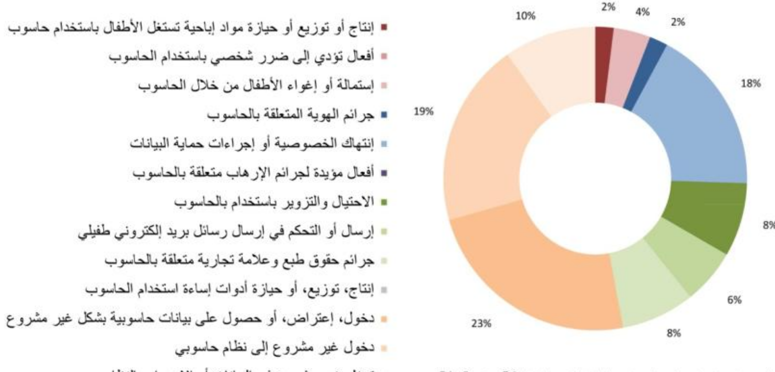


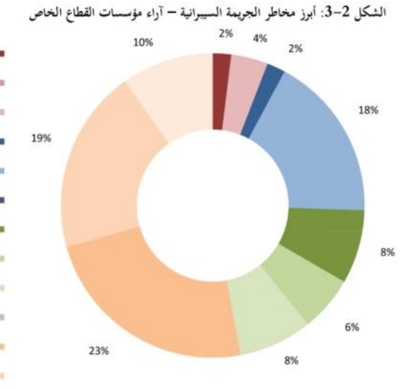
الشكل 2-2: أبرز مخاطر الجريمة السيبرانية – آراء الدول الأعضاء

المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 81. (رقم=59، 138)

الإيذاء وجود مستويات مختلفة في النفاذ غير المشروع للحاسوب، ومع ذلك لا توجد دائما اختلافات في نفس الاتجاه مثل ما تم تصوره من قِبَل هيئات إنفاذ القانون.

إن مسألة انتشار الجريمة السيبرانية وما يصاحبها من تهديد يختلف حسب الشخص الذي تم سؤاله، مما يبين





الشكل 2-3: أبرز مخاطر الجريمة السيبرانية – آراء مؤسسات القطاع الخاص

المصدر: استبيان دراسة الجريمة السيبرانية (القطاع الخاص). السؤال 56. (رقم=8، 51)

بصورة واضحة مقارنة النتائج من الدول والقطاع الخاص. عندما سُئلت هيئات إنفاذ القانون أي من أفعال

الجريمة السيبرانية يشكل الخطر الأبرز (من حيث الجسامة أو الخسارة أو الضرر)، فقد ماثَلَت الإجابات لتلك الردود المقدَّمة فيما يتعلق بالأعمال الأكثر شيوعا، مما يظهر تقريبا التوزيع المتساوي بين الأفعال المرتكبة بدافع مالي، والأفعال المتصلة بالمحتوى الحاسوبي، والأفعال المباشرة ضد نظم حاسوبية ومعلومات حاسوبية.

وعلى النقيض من ذلك، وكما كان متوقعا، فقد اعتبرت مؤسسات القطاع الخاص أن *الأفعال التي ترتكب ضد النظم الحاسوبية* تشكل تهديدا أكبر بكثير من الأنواع الأخرى من الجريمة السيبرانية. علاوة على ذلك، فقد اعتبرت هذه المؤسسات أن النفاذ أو التدخل غير المشروع، أو التسبب في إلحاق الضرر يمثل تهديدا أكبر من التهديد الذي يصاحب جميع الأنواع الأخرى من الجريمة السيبرانية. وهذا يعكس قلقا أساسيا يساور كيانات القطاع الخاص ويتمثل في الوصول إلى نظمها الحاسوبية، وكذلك الاطلاع على بياناتها الحاسوبية، وانتهاك سرية ونزاهة هذه النظم والبيانات.

أبرزت مؤسسات القطاع الخاص خلال جمع المعلومات الخاصة بهذه الدراسة، التهديدات والمخاطر الرئيسية التي تشكلها الجريمة السيبرانية، واشتمل ذلك على *"النفاذ غير المشروع إلى نظام حاسوبي وسرقة حقوق الملكية الفكرية"*، و*"اختراق موقعها الإلكتروني الخاص بالخدمات المصرفية"*، و*"تَسْرِيب المعلومات من قِبَل الموظفين"*، و*"هجمات حجب الخدمة"*.[1] وكما هو مبين أدناه، تعتبر كافة كيانات القطاع الخاص عُرْضَة للإيذاء الإلكتروني مما يمكن أن تكون التكاليف المتكبدة نتيجة هذا الإيذاء عالية.

إنتشار وتأثير أفعال الجريمة السيبرانية

يمكن تقسيم قياس انتشار أفعال الجريمة السيبرانية إلى: عموم السكان (أو المستهلك)، والإيذاء، وإيذاء المنظمات – مثل الشركات والمؤسسات الأكاديمية، وغيرها.[2]

الإيذاء الذي يلحق بالمستهلك – تعتبر مستويات الإيقاع الإجرامي بضحايا الجريمة السيبرانية بالنسبة لعموم السكان أعلى بكثير من تَأَذِّيهم بأشكال الجرائم التقليدية التي ترتكب دون الاتصال بالإنترنت – بالنسبة للسكان المعنيين المعرضين للخطر.[3] تتراوح معدلات الإيذاء الناشئ عن الجريمة السيبرانية بين 1 و17 في المائة من إجمالي مستعملي الإنترنت في 21 بلدا من مختلف أنحاء العالم، وتنحصر حالات تَأَذِّي عامة السكان بالجريمة السيبرانية في أربعة أعمال: الاحتيال المتعلق ببطاقات الائتمان عبر الإنترنت، وسرقة الهوية، والاستجابة لمحاولات التصيُّد الاحتيالي، والتعرُّض لحالات نفاذ غير مأذون به إلى حساب البريد الإلكتروني.[4] على عكس

---

[1] الاستبيان الخاص بدراسة الجريمة السيبرانية (القطاع الخاص). الأسئلة م50-52، والسؤال رقم 56.

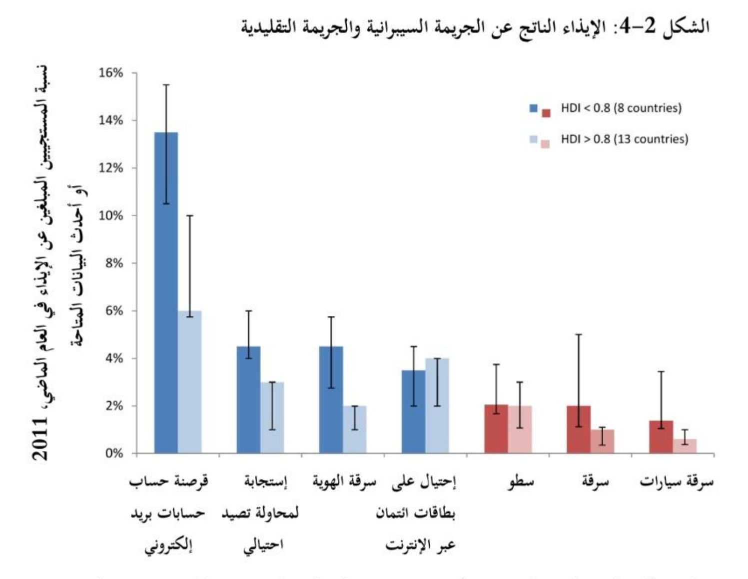
[2] يستعبد من نطاق هذه الدراسة إيذاء مؤسسات الحكومة.

[3] كل الأفراد معرضين ليكونوا عرضة لجريمة "تقليدية"، بالإضافة إلى تعرض كل مستخدمي الإنترنت للجريمة السيبرانية.

Symantec, 2012. Norton Cybercrime Report 2012. Research for the Norton Cybercrime Report was conducted[4] *independently by StrategyOne (now EdelmanBerland) through an online survey in 24 countries using identical questions translated into the primary language of each country. Interviews were conducted between 16 July 2012 and 30 July 2012. The margin of error for the total sample of adults (n=13,018) is +0.9 per cent at the 95 per cent level of confidence. Data from 3 countries in the Norton Cybercrime Report are excluded as national victimization data for conventional crime were not available. Victimization rates refer to 12 month prevalence of victimization.*

ذلك، تُظهر دراسات الإيذاء الاستقصائية أنَّ نسبة المتأذِّين بالجرائم "المعتادة"، مثل السطو والسلب وسرقة السيارات تتراوح ما بين 0.1 و13 في المائة، في البلدان الـ 21 نفسها، مع أن معدلات الغالبية العظمى لهذه الجرائم تحت نسبة 4 في المائة.[1] حيث يوجد عامل منفرد يبرر هذا الاختلاف، ويتمثل، على الأرجح، في طبيعة أفعال الجريمة السيبرانية المتعددة. ويمكن لفرد واحد أن يستهدف العديد من الضحايا، مثل أعمال التصيّد الاحتيالي أو "الهجوم التخميني" لكسر كلمة مرور للنفاذ غير المأذون به إلى حساب البريد الإلكتروني، بطريقة غير ممكنة في أشكال الجريمة التقليدية.

ويتمثل النمط الثاني للإيذاء الناشئ عن الجريمة السيبرانية في ارتفاع معدلات الإيقاع الإجرامي بضحايا الجريمة السيبرانية (على الأقل مستعملي الإنترنت في 21 بلدا من مختلف أنحاء العالم) بصفة عامة في تلك الدول مع تدني مستويات التنمية.



المصدر: إعداد مكتب الأمم المتحدة المعني بالمخدرات والجريمة: تقرير نورتن بشأن الجريمة السيبرانية واستطلاعات ضحايا الجريمة

فإذا قمنا بتقسيم الدول إلى مجموعتين: (المجموعة 1) فيها جَدْوَل قياس التنمية البشرية أقل من 0.8، و(المجموعة 2) أعلى بكثير من 0.8،[2] وهذا يبين ارتفاع معدلات الإيذاء في الدول الأقل تنمية (المجموعة 1) المتمثل في اختراق حساب بريد إلكتروني بصورة غير شرعية، سرقة الهوية، والاستجابة لمحاولة التصيد الاحتيالي. ويعتبر التأذِّي من الاحتيال المتعلق ببطاقات الائتمان عبر الإنترنت أعلى بقليل في المجموعة التي تضم الدول الأكثر تقدما. ويبين الشكل التالي متوسط معدلات الإيذاء الناشئ عن الأربعة أنواع من الجريمة السيبرانية، جنبا إلى جنب مع متوسط معدلات السطو والسرقة وسرقة السيارات للمجموعتين من البلدان.[3]

---

[1] تحليل مكتب الأمم المتحدة المعني بالمخدرات والجريمة لنتائج الدراسة الدولية والوطنية الاستقصائية المعنية بالإيذاء الناشئ عن الجريمة السيبرانية. تشير معدلات الإيذاء إلى 12 شهر من انتشار الإيذاء.

[2] يتم احتساب المتوسطات على أساس متوسطات معدل الإيذاء لكل مجموعة على حدة. توضح القضبان الرُبيع العلوي والسفلي.

[3] المجموعة (1): جدول التنمية البشرية يشير إلى 0.69، متوسط 0.7، المجموعة (2): جدول التنمية البشرية يشير إلى 0.89، متوسط = 0.90، يوضح جدول التنمية البشرية مَجْمُوع قياس التنمية الاقتصادية والاجتماعية. أنظر: /http://hdr.undp.org/en/statistics/hdi

هذا، ويوجد اتساق بين نموذج ارتفاع معدل الإيذاء الناتج عن الجريمة السيبرانية في الدول الأقل نموا وبين ارتفاع معدلات الجريمة التقليدية في هذه الدول بشكل عام. وفيما يتعلق بالجريمة التقليدية، فإن هذه الاختلافات ترجع إلى عدد من العوامل، منها عدم المساواة في الدخل، والتحديات الاقتصادية، وزيادة معدل الشباب من المجموع الكلي للسكان، والتَمَدُّن، وتاريخ من الصراع، وانتشار الأسلحة النارية، وضعف التمويل المخصص لنظم العدالة الجنائية.[1] وتتسم بعض من هذه العوامل بأهمية أدنى بالنسبة للجريمة السيبرانية. ومع ذلك، رُبَّمَا تشكل العوامل الأخرى؛ مثل الضغوط الاقتصادية والديموغرافية، جزءا من معادلة الجريمة السيبرانية. ويمكن من حيث المبدأ، أن يكون ضحايا الجريمة السيبرانية في الدول الأقل نموا هدفا للجناة من أي مكان في العالم، ومع ذلك؛ تساهم العوامل المتعلقة بالثقافة المحلية واللغة في أن يكونوا هدفا للجناة من بلدهم، مما يشكل عوامل خطر متعلقة بالجناة المحليين. بالإضافة إلى ذلك؛ غالبا ما يواجه مستخدمو الإنترنت في الدول النامية تحديات انخفاض الوعي بالأمن السيبراني، مما يجعلهم بصفة خاصة عرضة للجرائم، مثل النفاذ غير المأذون به للحاسوب، والتصيد الاحتيالي وسرقة الهوية.[2] وعلى الرغم مما أظهرته دراسات الإيذاء الاستقصائية، فإن هذا النمط أيضا يتوافق مع حقيقة مؤداها عدم اعتبار سلطات إنفاذ القانون، في الدول الأقل نموا، النفاذ غير المشروع أحد أفعال الجريمة السيبرانية كما هو شائع بصفة خاصة.[3]

وعلى النقيض من ذلك، تُظهر حالات الاحتيال المتعلق ببطاقات الائتمان عبر الإنترنت نمطا معاكسا، حيث تعتبر معدلات الإيذاء الناتج عن هذه الجريمة متساوية بشكل كبير وربما أعلى بقليل في الدول الأكثر تقدما. فمن المرجح، ارتباط هذا النمط جزئيا بالاختلافات في ملكية بطاقات الائتمان واستعمالها عبر الإنترنت، علاوة على الاختلافات في استهداف الضحية والذي يرجع إلى الوُقُوف على ماهية الهدف الأفضل. فعلى سبيل المثال؛ يعلل مكتب الشرطة الأوروبي (اليوروبول) ارتفاع مستويات حالات الاحتيال المتعلق ببطاقات الائتمان عبر الإنترنت (البطاقة ليست موجودة) التي تؤثر على بطاقات الائتمان الخاصة بالاتحاد الأوروبي، كنتيجة لانتهاكات البيانات والمعاملات التجارية غير المشروعة.[4]

يحمل انتشار معدلات إيذاء الجريمة السيبرانية للمستهلك في طياته تكاليف مالية كبيرة سواء أكان ذلك بصفة مباشرة أو غير مباشرة، وتتجسد التكاليف المباشرة وغير المباشرة في الأموال المسحوبة من حسابات الضحية، أو الوقت والجهد المستغرق لإعادة أوراق اعتماد الحساب المصرفي، أو إصلاح نظم الحاسوب، بالإضافة إلى التكاليف الثانوية مثل السحب على المكشوف. وتتمثل النفقات غير المباشرة في المقابل النقدي للخسائر التي يتكبدها المجتمع نتيجة وجود ظاهرة جريمة سيبرانية مُعَيّنة بشكل عام. ويتمخض عن هذه

---

[1] أنظر على سبيل المثال: مكتب الأمم المتحدة المعني بالمخدرات والجريمة 2005. "الجريمة والتنمية في أفريقيا"، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة 2007، الجريمة والتنمية في أمريكا الوسطى.

[2] أنظر على سبيل المثال:
Tagert, A.C., 2010. *Cybersecurity Challenges in Developing Nations*. Dissertation. Paper 22; and Grobler, M., et al., 2010. Evaluating Cyber Security Awareness in South Africa. *In*: Ottis, R. (ed.) 2011. *The Proceedings of the 10th European Conference on Information Warfare and Security*. Talinn: Cooperative Cyber Defence Centre of Excellence.

[3] أنظر أعلاه، على سبيل المثال ما يتعلق بالمعلومات الظاهرة في الشكل 2-4.

[4] Europol, 2012. *Situation Report. Payment Card Fraud in the European Union. Perspective of Law Enforcement Agencies*

النفقات غير المباشرة فقدان الثقة في الخدمات المصرفية عبر الإنترنت وانخفاض إقبال الأفراد على الخدمات الإلكترونية. فالتكلفة الإجمالية التي يتحملها المجتمع نتيجة الجريمة السيبرانية قد تتضمن أيضا "تكاليف الدفاع" عن منتجات وخدمات الأمن السيبراني، علاوة على تكاليف الكشف عن الاحتيال والجهود المبذولة لإنفاذ القانون.[1]

وأشارت إحدى التقارير إلى أن متوسط الخسائر المباشرة التي تَحَمّلها ضحايا الجريمة السيبرانية من المستهلكين في 24 دولة من جميع دول العالم يقدر بما بين 50 و850 دولارا أمريكيا كنتيجة لإحدى الجرائم السيبرانية التي عانت منها في سنة واحدة،[2] حيث اشْتَمَل نحو 40 في المائة من هذه التكاليف على خسارة مالية بسبب الاحتيال، وحوالي 20 في المائة متجسدين في فقد الهوية أو سرقتها، وما يقرب من 25 في المائة متمثلين في إجراء أعمال صيانة للنظم الحاسوبية، والنسب الباقية تمثلت في مواجهة الجريمة السيبرانية أو الخسائر المالية الأخرى.[3] ويوضح الشكل 2-5 متوسط خسائر الدول حسب هذه الدراسة.[4] وترجع الاختلافات في متوسط الخسائر المعلن عنها عبر الدول إلى عدد من العوامل، منها؛ نوع الإيقاع الإجرامي بضحايا الجريمة السيبرانية، وفعالية تدابير الأمن السيبراني، ونطاق استخدام الضحية للإنترنت لإجراءات عمليات مصرفية أو الدفع مباشرة على الإنترنت. هذا ولا تتضمن التكاليف التي يقدرها الضحايا أنفسهم تلك المتعلقة بالتكاليف غير المباشرة وتكاليف الدفاع.

الشكل 2-5: التكاليف التقديرية للجريمة السيبرانية التي تحملها المستهلك، حسب الدولة

متوسط التكلفة/الخسارة بالدولار الأمريكي
تقرير نورتن بشأن الجريمة السيبرانية، متوسط التكلفة لكل واقعة
الحسابات وفق أندرسون وآخرون، ومتوسط نصيب الفرد من الخسائر
$450.00 $400.00 $350.00 $300.00 $250.00 $200.00 $150.00 $100.00 $50.00 $0.00
CO JP TR RU SE DK MX CA CN ZA IN SA GB DE BR AE US FR AU

المصدر: تقرير نورتن بشأن الجريمة السيبرانية ومكتب الأمم المتحدة المعني بالمخدرات والجريمة

[1] أنظر على سبيل المثال:
Anderson, R., et al., 2012. Measuring the Cost of Cybercrime. *11th Annual Workshop on the Economics of Information Security*, WEIS 2012, Berlin, 25-26 June 2012

[2] Symantec, 2012. *Norton Cybercrime Report 2012* وكان السؤال الذي طرحته الدراسة على كل الأشخاص وضحايا الإيذاء الناشئ عن الجريمة السيبرانية في الأشهر الـ 12 الماضية يتعلق ما هي مقدار الخسارة المالية على مدى الأشهر الـ 12 الماضية بسبب الجريمة السيبرانية. وقد طُلب من المجيبين أن يُفكروا في مقدار إجمالي الخسارة المالية، بما في ذلك أي مبالغ مالية قد سرقت وكذلك تكاليف إصلاح نظم الحاسوب ومواجهة الجريمة السيبرانية. وذكرت بيانات بشأن الخسارة المالية الإجمالية السنوية بالعملة المحلية وتحويلها إلى الدولار الأمريكي للمقارنة عبر الحدود الوطنية

[3] المرجع السابق

[4] يستبعد الشكل الدول إذا كان تقدير الخطأ المعياري أكبر من 0.5، كان هذا هو الحال على وجه الخصوص لبعض من تقديرات الخسائر الكبيرة المبلغ عنها.

وبالمقارنة، يُظهر الشكل إجمالي التكاليف المقدرة للجريمة السيبرانية (بما في ذلك التكاليف المباشرة وغير المباشرة، وكذلك تكاليف الدفاع) لِكُلّ شخص بناء على الحسابات الواردة في المواد المطبوعة المتوفرة،[1] غير أنه لا يجب مقارنة المستويات القَطْعِيّة للشكلين، حيث يمثل الشكل الأول متوسط التكاليف المباشرة التي تتحملها كل ضحية، بينما يوضح الآخر التكاليف الإجمالية مقسومة على مجموع السكان. ومع ذلك تظهر بعض النماذج النسبية بعض درجات التطابق، بيد أنه إذا طَرَأت اختلافات كبيرة، فإن إحدى العوامل المسَاعِدة قد تحدث اختلافات في اخْتِراق الإنترنت وتوزيع التكاليف على المجتمع، حيث إن تقسيم الخسائر الناتجة عن الجريمة السيبرانية على عدد كبير من السكان لا يتصلون جميعهم بالإنترنت سيكون له تأثير ظاهري على خفض متوسط الخسائر لكل شخص، كما هو الحال في البلدان الأقل نموا، على سبيل المثال. ويظهر هذا التأثير بوضوح في الشكل؛ في حالة وجود عدد من البلدان النامية، حيث لا يتطابق بشكل جيد النموذج الخاص بإجمالي تكلفة الخسائر المقدرة لكل شخص مع نموذج الخسائر المباشرة للمستهلك المبلغ عنها. وفي مثل هذه الحالات، فإن النموذج الأساسي يعتبر، على الأرجح، بمثابة النموذج الأقرب الذي وضحته الدراسات الاستقصائية المعنية بالضحية. وعلى العكس من ذلك، ففي حالة الدول المتقدمة جدا حيث تنخفض تكاليف المستهلك جدا بشكل نسبي، فإن إجمالي تكاليف الخسائر المقدرة لكل فرد تعتبر أعلى من المتوقع من خسائر المستهلك وحده، في إشارة إلى التكاليف المباشرة وتكاليف الدفاع الكبيرة والإضافية في هذه الدول.

الإيذاء الذي يلحق بالقطاع الخاص – تعتبر تقنيات الجريمة السيبرانية بمثابة ثورة من الاحتيال التقليدي والجرائم ذات الدافع المالي المرتكبة ضد كيانات القطاع الخاص. فلقد أدت إمكانيات التصاعد الإجرامي المتمثل ليس فقط في الاحتيال على أحد المؤسسات، وإنما أيضا في الحصول على معلومات شخصية ومالية مخزنة من خلال اختراق البيانات إلى ارتفاع وتيرة خطر الجريمة السيبرانية في القطاع الخاص،[2] وفي نفس الوقت، تقدم زيادة استخدام المخترعات مثل الحوسبة السحابية مزيجا من فوائد الأمن السيبراني وتحديات له.[3]

---

1 UNODC calculations from Anderson, R., *et al.*, 2012. *Measuring the Cost of Cybercrime*. Global estimates from this source were attributed to countries based on GDP share

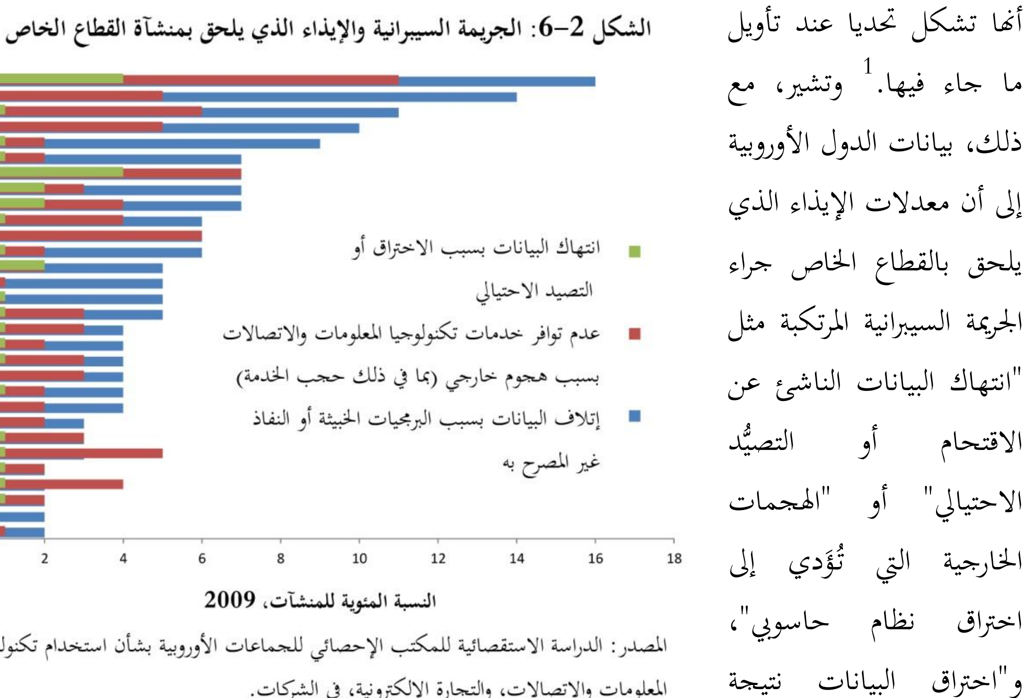
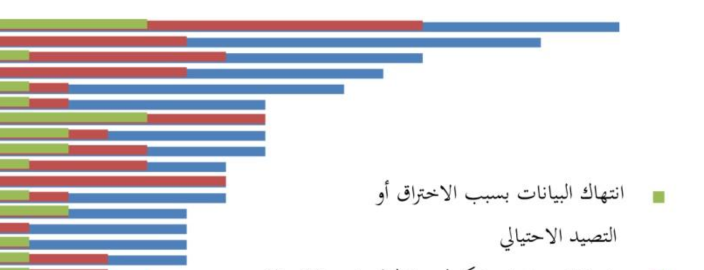
2 أُنظر على سبيل المثال: KPMG, 2011. *The e-Crime Report 2011*

قد أبلغ أكثر من نصف صانعي القرار الأمني في المنشآت أن المستوى العام لمخاطر الجريمة الإلكترونية التي يواجهونها قد تزايدت خلال الأشهر الـ 12 الماضية، بيد أن 6 في المائة فقد أبلغوا بأنها قد انخفضت. وذكر اليوروبول أن التحقيقات أظهرت أن المصادر الرئيسية للبيانات غير الشرعية في عمليات الاحتيال دون وجود بطاقة ائتمانية كانت بيانات التجار المخترقة، وكذلك بيانات مراكز معالجة البطاقات، فغالبا ما يتيسر ذلك من قبل المطّلعين أو البرامج الضارة. (Europol, 2012. *Situation Report. Payment Card Fraud in the European Union. Perspective of Law Enforcement Agencies*).

3 PricewaterhouseCoopers, 2012. *Eye of the storm. Key findings from the 2012 Global State of Information Security Survey*

يعتبر الحصول على بيانات مؤثُوقة بشأن الإيذاء الذي يلحق بالقطاع الخاص من الأمور الصعبة، كما أنها تشكل تحديا عند تأويل ما جاء فيها.[1] وتشير، مع ذلك، بيانات الدول الأوروبية إلى أن معدلات الإيذاء الذي يلحق بالقطاع الخاص جراء الجريمة السيبرانية المرتكبة مثل "انتهاك البيانات الناشئ عن الاقتحام أو التصيُّد الاحتيالي" أو "الهجمات الخارجية التي تُؤَدي إلى اختراق نظام حاسوبي"، و"اختراق البيانات نتيجة اقتحام النظام الحاسوبي بصورة غير شرعية"، تعتبر قابلة للمقارنة على نطاق واسع مع النفاذ غير المشروع للحاسوب والتصيُّد الاحتيالي، وحالات الاحتيال المتعلق ببطاقات الائتمان عبر الإنترنت التي عانى منها المستهلكون. ما بين 2 و16 في المائة من المنشآت في أوروبا، على سبيل المثال، عانت من تلف البيانات بسبب البرامج الضارة أو النفاذ غير المصرح به خلال العام 2010،[2] حيث يرجع تلف البيانات إلى النفاذ غير المصرح به بشكل متكرر وبصورة أكبر من عدم توفر خدمات تكنولوجيا المعلومات والاتصالات بسبب الهجمات الخارجية (ما بين 1 و11 في المائة)، والتي حدثت تباعا بشكل أكثر تواترا من اختراق البيانات بسبب البرامج الضارة أو التصيد الاحتيالي (ما بين صفر وأربعة في المائة).

الشكل 2–6: الجريمة السيبرانية والإيذاء الذي يلحق بمنشآة القطاع الخاص

المصدر: الدراسة الاستقصائية للمكتب الإحصائي للجماعات الأوروبية بشأن استخدام تكنولوجيا المعلومات والاتصالات، والتجارة الإلكترونية، في الشركات.

الشكل 2–7: الأذى الذي يلحق بالمنشآت حسب الحجم

منشآت صغيرة (10–49 شخص)
منشآت متوسطة (50–249 شخص)
منشآت ضخمة (فوق 250 شخص)

النسبة المئوية للمنشآت التي عانت من تلف البيانات بسبب برمجيات خبيثة أو دخول غير مرخص به

المصدر: الدراسة الاستقصائية للمكتب الإحصائي للجماعات الأوروبية بشأن استخدام تكنولوجيا المعلومات والاتصالات، والتجارة الإلكترونية، في الشركات.

بالرغم من ذلك؛ فإن

[1] أنظر الملحق الثاني (قياس الجريمة السيبرانية).

[2] Eurostat, 2011. *Community survey on ICT usage and e-commerce in enterprises*. The survey covered 149,900 enterprises out of 1.6 million in the EU27.

الكثير يبقى مرهونا بالطريقة التي طرحت بها الأسئلة، وتصورات المجيبين لما يشكل "خرقا للبيانات" أو "الاقتحام"، أو "عدم توافر خدمات تكنولوجيا المعلومات والاتصالات" أو "البرامج الضارة". بيد أن إحدى الدراسات الاستقصائية التي تناولت كيانات القطاع الخاص في خمس دول تشير، على سبيل المثال، إلى ارتفاع معدلات الإيذاء الذي يلحق بالمنشآت بصورة كبيرة للغاية، مثلا هناك ما بين 1.1 و1.8 *"هجوم سيبراني ناجح كل أسبوع على منشأة تم استطلاعها"*.[1] وفي الغالب، فإن هذه النتائج تتأثر بشكل كبير ليس فقط في التصورات حول ما يشكل "الهجوم السيبراني" على إحدى المنشآت،[2] وإنما أيضا بحجم البنية التحتية الحاسوبية للمنشأة المعرضة للهجوم. وجدير بالذكر، أن هذه الدراسة الاستقصائية ركزت بشكل خاص، على سبيل المثال، على المنشآت التي لديها أكثر من 1,000 "مقاعد للمنشأة" – أي الإتصالات المباشرة مع الشبكة وأنظمة المنشأة.[3]

في الواقع، إن خطر الجريمة السيبرانية البالغ الذي تواجهه المنشآت الكبرى تؤكده أيضا بيانات القطاع الخاص الأوروبي. وتعتبر نسبة المنشآت في أوروبا التي تعاني من تلف البيانات بسبب البرامج الضارة أو النفاذ غير المشروع أكبر بالنسبة للمنشآت الكبرى (أكثر من 250 شخص) (2–27 في المائة)، من المنشآت المتوسطة (50–249 شخص) (2–21 في المائة)، والتي تعتبر بدورها أكبر من المنشآت الصغيرة (10–49 شخص) (1–15 في المائة).

بالإضافة إلى "تعرض السطح الخارجي للهجوم"، يمكن أن ترتبط هذه الاختلافات أيضا بتصور لدى مرتكبي الجريمة السيبرانية بأن المنشآت الكبرى تمثل أهدافا ذات قيمة كبيرة. ويمكن أن يعزى الأمر أيضا، من ناحية ثانية، إلى كون قدرة المنشآت الصغيرة والمتوسطة، في المقام الأول، أقل على تحديد الهجمات الإلكترونية. وأخيرا، فإن نحو 65 في المائة من المنشآت الكبرى، على سبيل المثال، لديها سياسة محددة بشأن تكنولوجيا المعلومات والاتصالات بصفة رسمية، مقارنة مع المنشآت المتوسطة التي تبلغ فيها النسبة 43 في المائة، و22 في المائة فقط من الشركات الصغيرة التي لديها نفس السياسة.[4]

الأدوات الجنائية – "البوتنت"

تتجسد السمة المميزة اليوم لمشهد الجريمة السيبرانية في الاستخدام الشامل لأدوات إساءة استخدام الحاسوب عبر مجال من الجرائم السيبرانية. ويعتبر "البوتنت" (مصطلح مشتق من كلمتين "روبوت" و"شبكة") أحد الأدوات المستخدمة في ارتكاب الجريمة السيبرانية، ويتألف من شبكة مترابطة من أجهزة الحاسوب يتم التحكم فيها عن بعد؛ وبصفة عامة، فإن هذه الأجهزة مخترقة ببرمجيات خبيثة تحول الأنظمة المصابة إلى ما

[1] HP/Ponemon, 2012. *Cost of Cybercrime Study AU, DE, JN, GB and US*

[2] Survey results are thus more reliable where experience of a particular, defined event, is asked about. See UNODC/UNECE, 2010.*Manual on Victimization Surveys.*

[3] المرجع السابق

[4] Eurostat, 2011. Statistics in Focus 7/2011. ICT security in enterprises, 2010

يعرف بـ "روبوت" أو "بوت" أو "زومبي".[1] وفي أغلب الأحيان، يجهل الملاك الشرعيون لهذه الأجهزة حقيقة الإصابة التي تتم عن طريق الحواسيب المدمرة ضمن شبكة الروبوت المتصل بأجهزة الحاسوب التي يتحكم فيها الجناة (وتعرف باسم خوادم القيادة والسيطرة)، أوعن طريق تحميل برمجيات إضافية من الحواسيب المدمرة الأخرى لكي تتلقى التعليمات وترسل المعلومات المجمعة من الجهاز المصاب مرة أخرى.

نظرا لأنه يمكن استخدام شبكات الروبوت في عدد من الأفعال – منها هجمات حجب الخدمة الموزعة، إرسال رسائل البريد الإلكتروني الطفيلي، سرقة المعلومات الشخصية، استضافة المواقع الإلكترونية الخبيثة، ونقل حملات من البرمجيات الخبيثة[2] – فهي تمثل الأداة الرئيسية المختارة في ارتكاب الجريمة السيبرانية. وأكد عدد من البلدان على زيادة استخدام شبكات الروبوت في ارتكاب الجريمة السيبرانية خلال الخمس سنوات الماضية.[3] ومن وجهة نظر القانون الجنائي؛ يتيح تركيب البرمجيات الخبيثة في نظام الحاسوب الشخصي أو المملوك لإحدى المنشآت النفاذ غير المشروع للنظام الحاسوب، و/أو اختراق البيانات بصورة غير قانونية، أو اختراق النظام.[4] ويعتبر إنتاج برمجيات الروبوت، أو بيعها، أو حيازتها، أو توزيعها بمثابة جريمة جنائية، وذلك في الدول التي تجرم سوء استخدام الأدوات الحاسوبية. بالإضافة إلى ذلك، قد يشكل استخدام شبكة الروبوت في ارتكاب مزيد من الأفعال الإجرامية مجموعة من الجرائم، مثل النفاذ غير المشروع، أو اعتراض، أو الحصول على البيانات الحاسوبية، واستخدام الحاسوب في الاحتيال، واستخدام الحاسوب في جرائم الهوية، وإرسال أو التحكم في إرسال الرسائل الطفيلية.[5]

رسم خريطة خوادم القيادة والسيطرة، والحواسيب المدمرة (الزومبي) – يُظهر أن شبكة الروبوت تسهل ارتكاب مجموعة كبيرة من أفعال الجريمة السيبرانية، فالوُقُوف على مكان ونطاق خوادم التحكم ورقابة شبكة الروبوت والحواسيب المدمرة يقدم أحد النهج الهامة لوصف "الجريمة السيبرانية العالمية". وتشير التقديرات إلى أن أكثر من مليون عنوان فريد من عناوين بروتوكولات الإنترنت يعمل على الصعيد العالمي كخادم لشبكة الروبوت للتحكُّم في الشبكات الحاسوبية ومراقبتها، في عام 2011.[6] ويوضح الشكل 2-8 والشكل 2-9 عملية توزيع التحكم في شبكات الحواسيب ومراقبتها المحددة[7] في عام 2011 و2012 لكل 100,000 من إقليم

[1] OECD, 2008. *Malicious Software (Malware). A Security Threat to the Internet Economy.* DSTI/ICCP/REG(2007)5/FINAL. 28 April 2008.

[2] Hogben, G. (ed.) 2011. *Botnets: Detection, Measurement, Disinfection and Defence.* European Network and Information Security Agency(ENISA

[3] الاستبيان الخاص بدراسة الجريمة السيبرانية، السؤال رقم 84

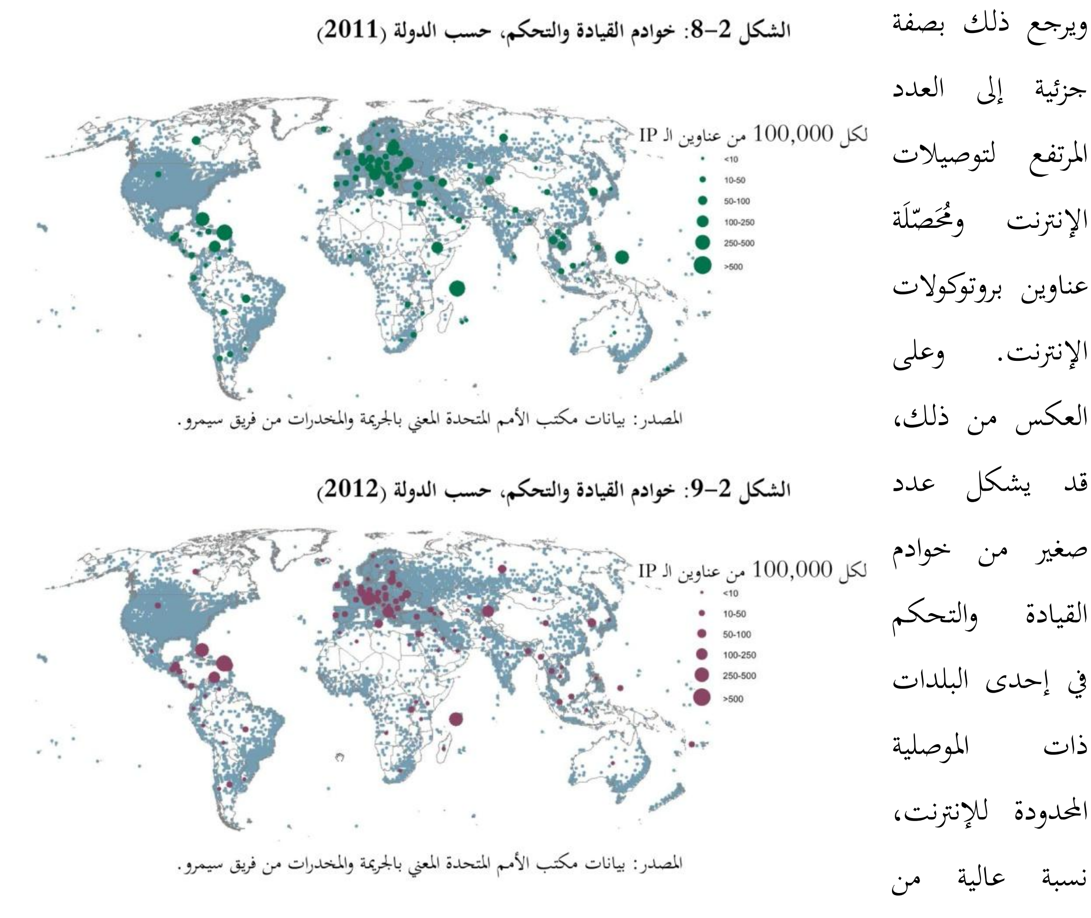
[4] أنظر الملحق الأول (وصف أفعال الجريمة السيبرانية)، وأنظر أيضا: NATO Cooperative Cyber Defence Centre of Excellence and ENISA, 2012. *Legal Implications of Countering Botnets.*

[5] المرجع السابق.

[6] استندت التقديرات إلى البيانات الواردة من فريق سيمور.

[7] تتوافق بيانات عناوين بروتوكولات الإنترنت المحددة في أي وقت خلال 2011 أو 2012، حيث تعمل بمثابة IRC (نقل المحادثات عبر الإنترنت) أو HTTP (ميثاق نقل النص الفائق) لخادم لشبكة الروبوت للتحكُّم في شبكات الحواسيب ومراقبتها

عناوين بروتكولات الإنترنت.[1] بالإضافة إلى مجموعة خوادم القيادة والتحكم في أوروبا الشرقية، فإن عددا منها ذو صلة بالعدد الإجمالي لإقليم عناوين بروتوكولات الإنترنت في غرب ووسط وجنوب شرق آسيا، وكذلك في أمريكا الوسطى ومنطقة الكاريبي. وبينما يمثل العدد المطلق لخوادم القيادة والتحكم في بلدان أمريكا الشمالية وأوروبا الغربية وشرق آسيا نسبة عالية، إلا أن معدلات القيادة والتحكم في هذه الدول تعتبر منخفضة نسبيا، ويرجع ذلك بصفة جزئية إلى العدد المرتفع لتوصيلات الإنترنت ومُحَصّلَة عناوين بروتوكولات الإنترنت. وعلى العكس من ذلك، قد يشكل عدد صغير من خوادم القيادة والتحكم في إحدى البلدان ذات الموصلية المحدودة للإنترنت، نسبة عالية من القيادة والتحكم – على النحو نفسه الذي يمكن أن يشكل فيه عدد قليل من الجرائم في جزيرة صغيرة معدلا عاليا من الجريمة.



الشكل 2–8: خوادم القيادة والتحكم، حسب الدولة (2011)

المصدر: بيانات مكتب الأمم المتحدة المعني بالجريمة والمخدرات من فريق سيمرو.

الشكل 2–9: خوادم القيادة والتحكم، حسب الدولة (2012)

المصدر: بيانات مكتب الأمم المتحدة المعني بالجريمة والمخدرات من فريق سيمرو.

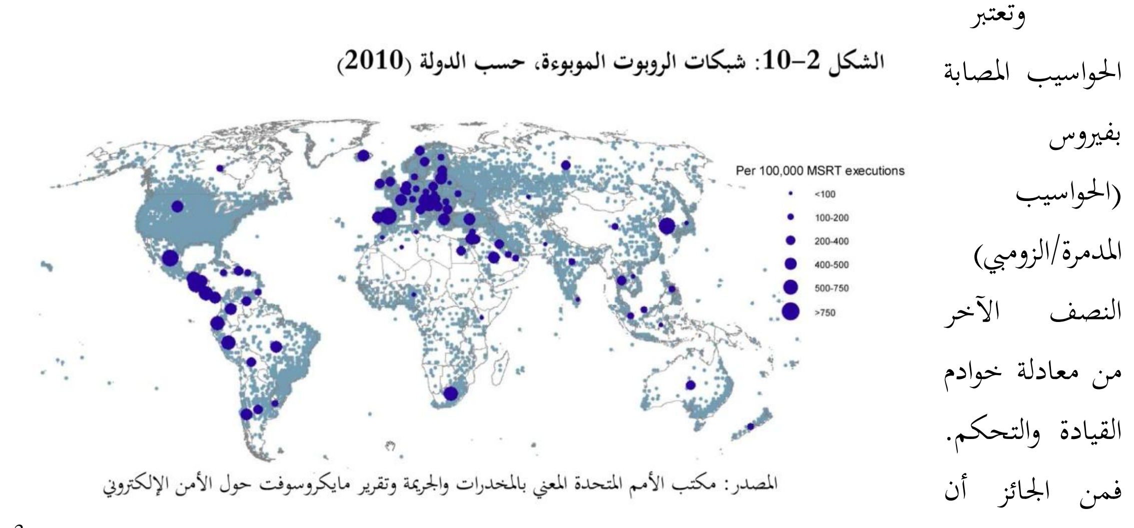
من المستقر أن التوزيع العالمي لخوادم القيادة والتحكم لا يرتبط بالضرورة مع أماكن الجناة، أو "رعاة" الروبوت الذين يتحكمون في خوادم القيادة والتحكم، ويسخّرون شبكات الروبوت الخاصة بهم لأغراض الربح. ففي أغلب الأحيان، يتم نقل أماكن خوادم القيادة والتحكم لتجنب تحديد موقعها، ويمكن أن تشتمل على

---

[1] البيانات الواردة من فريق سيمور. معدلات التحكم في شبكة الإنترنت ومراقبتها في كل دولة مَرْسُوم باللون أخضر لـ(2011)، و بلون أُرْجُوَانِيّ لـ (2012)، جنبا إلى جنب مع الموقع الجغرافي لكل عناوين بروتوكولات الإنترنت العالمية بلون أزرق (بيانات واردة من ماكس ميند). شبكة التحكم في شبكة الإنترنت ومراقبتها المحددة المرسومة لكل 100,000 من عناوين برتوكولات الإنترنت في الدولة تسمح بقدر من المقارنة مع الجرائم المرتكبة عبر الحدود الوطنيةأكبر من العدد المطلق لشبكات التحكم في شبكة الإنترنت ومراقبتها. ويخضع الموقع الجغرافي للتحكم في عناوين بروتكولات الإنترنت ورقابتها إلى عدد من التحديات، منها استخدام اتصالات الخادم الوكيل. على الرغم من أن المكان على المستوى القطري يعتبر مقبولا بصفة عامة.

استخدام أنظمة الكشف "البسيطة".[1] وفي ضوء ذلك، فإن راعي شبكة الروبوت ليس في حاجة إلى أن يكون قريبا جغرافيا من خوادم التحكم والقيادة، وبرغم ذلك؛ فإنه من الممكن أن توجد روابط محلية، ولاسيما الروابط اللغوية، بين الجناة وبعض من مقدمي الخدمات، بما في ذلك من يطلق عليهم مقدمي خدمات "الاستضافة المضادة للرصاص".[2] ويشير القسم المعني بـ (مرتكبي الجريمة السيبرانية) في هذا الفصل، على سبيل المثال، إلى وجود مَراكز لمرتكبي الجرايمة السيبرانية في أوروبا الشرقية، ويتطابق ذلك مع نموذج معدلات القيادة والتحكم العالية في هذه المناطق الفرعية.

الشكل 2–10: شبكات الروبوت الموبوءة، حسب الدولة (2010)



المصدر: مكتب الأمم المتحدة المعني بالمخدرات والجريمة وتقرير مايكروسوفت حول الأمن الإلكتروني

وتعتبر الحواسيب المصابة بفيروس (الحواسيب المدمرة/الزومبي) النصف الآخر من معادلة خوادم القيادة والتحكم. فمن الجائز أن تكون سبعة ملايين، على الأقل، من أجهزة الحاسوب جزءا من شبكة روبوت، وذلك على الصعيد العالمي،[3] بيد أن هناك تقديرات أخرى تشير إلى ارتفاع هذا العدد بكثير.[4] يظهر الشكل 2–10 التوزيع التقريبي لهذه الإصابات حسب الدولة.[5]

يبين توزيع الإصابة شكلا مختلفا عن ذلك الخاص بخوادم القيادة والتحكم، حيث تَتجَمَّعَ الحواسيب المدمرة بشكل أكبر في أوروبا الغربية (على العكس من شرق أوروبا فيما يتعلق بخوادم القيادة والتحكم)، ويُظهر

---

[1] بالإضافة إلى شبكات الروبوت الندية في الآونة الأخيرة، حيث يمكن لأي حاسوب مدمر أن يكون عميل أو خادم، وذلك للحيلولة دون الحاجة إلى خادم لشبكات الروبوت لتحميل برامج أو تلقى تعليمات.

[2] وفيما يتعلق بمقدمي الاستضافة، أُنظر على سبيل المثال:
HostExploit and Group IB, 2012. *Top 50 Bad Hosts and Networks Report.*

[3] UNODC calculations based on Microsoft, 2010. *Microsoft Security Intelligence Report*. Volume 9. Figure as of first half 2010. This estimate is of the same order of magnitude as that of Symantec, 2011. *Internet Security Threat Report. 2011*. Volume 17 (estimate of 4.5 million for 2010).

[4] أُنظر على سبيل المثال: Acohido, B., 2010. Are there 6.8 million –or 24 million– botted PCs on the Internet? *The Last Watchdog.* Available at: http://lastwatchdog.com/6-8-million-24-million-botted-pcs-internet/

[5] تُرسم الحواسيب المدمرة باعتبارها شبكة روبوت تحمل عدة إصابات محددة لكل 100,000، حيث تعملأداة ميكروسوفت علىإزالة البرمجيات الخبيثة. البيانات الواردة من شركة مايكروسوفت 2010. تقرير مايكروسوفت بشأن الاستخبارات الأمنية. الجزء 9. تتناول المنهجية المستخدمة تلك الأجهزة فقط بنظام التشغيل ويندوز وتعمل على تحديثه (تقريبا 600 مليون جهاز في جميع أنحاء العالم) وتحدد فقط أكثر الفيروسات التي تحملها شبكة الروبوت. ومع ذلك، فقد وجدت المنهجيات المستقلة أن هناك تشابه في مستويات الإصابة عندما تحسب على أساس كل بلد على حدة. للمزيد، أُنظر على سبيل المثال:
van Eeten, M.J.G. *et al.*, 2011. *Internet Service Providers and Botnet Mitigation. A Fact-Finding Study on the Dutch Market.* Faculty of Technology Police and Management, Delft University of Technology.

هذا التجمع معدلات جسمية من الإصابة في أمريكا الشمالية وأمريكا الوسطى والجنوبية، وكذلك بعض الدول في شرق آسيا. ويهدف هذا التوزيع إلى بيان ماهية الدول ذات العدد الكبير النشط من مستخدمي الحاسوب.

تواجه التقديرات الإجمالية للحواسيب المدمرة وحجم شبكات الروبوت قيودا كبيرة. بيد أن هناك تمييزين هامين فيما يتعلق بالمنهجية، يؤثران على التقديرات ويتضمنان شبكة روبوت "البصمة" مقابل "عدد الحواسيب الإجمالي بشكل مباشر"،[1] وقياس الحواسيب المدمرة "عناوين بروتكولات الإنترنت" مقابل "الأجهزة الفريدة من نوعها".[2] وفي هذا الصدد؛ تجدر الإشارة إلى أن (بسبب العوامل المنهجية) التقدير الخاص بالقيادة والتحكم أعلاه يتَعَلّق بعنوان فريد من عناوين بروتكولات الإنترنت، أما الحواسيب المدمرة فهي تخصّ أجهزة الحاسوب. ومن ثم ليس من اليسير المقارنة بين الشكلين العالميين.

في الواقع، عندما يتعلق الأمر بتقديرات حجم شبكة الروبوت الفردية، فإن وُجُود تقنية مُتَداوَلة لقياس الحواسيب المدمرة لعناوين بروتوكولات الإنترنت الفريدة على مدى فترات طويلة من الزمن يعتبر، من المرجح، مغالاة في التقدير بشكل ملحوظ لأعداد الأجهزة المصابة.[3] وبينما تظل قياسات حجم شبكات الروبوت مثيرة للجدل، تشير الدلائل إلى "نجاح" نموذجي لرعاة الروبوت في السيطرة على مجموعة من أجهزة الحاسوب المصابة والتي تبلغ عشرات أو مئات الآلاف من الأجهزة، أو بالأحرى كما ذكر؛ "الملايين" من الأجهزة.[4] وعلى هذا الأساس، يعتبر العدد الإجمالي لشبكات الروبوت التجارية الإجرامية الكبيرة عالميا صغيرا نسبيا على الأرجح.

---

[1] ترتبط الحواسيب المدمرة بشبكات الروبوت وتتركها بصفة مستمرة، مثلما تُصاب الأجهزة الحديثة ويتم إزالة فيروس الحواسيب المدمرة الموجودة. بالإضافة إلى ذلك، قد تعاني الأجهزة المصابة من العديد من الإصابات أو تنتقل بصفة مؤقتة من شبكة روبرت إلى شبكة أخرى. أُنظر على سبيل المثال: (Abu Rajab, M., et al., 2007. My Botnet is Bigger than Yours (Maybe, Better than Yours): لماذا تبقى حجمالتقديرات محلا للتحدي. وقائع المؤتمر الأول حول ورشة العمل الأولى حول الموضوعات الساخنة في فهم ماهية شبكات الروبوت.(بيركلي، كاليفورنيا: جمعية يوسنت). تشير شبكة الروبوت (البصمة) إلى العدد الإجمالي الكلي للأجهزة التي قد اكتشفت إصابتها مع مرور الوقت، أما شبكة الروبوت (السكان بشكل مباشر) فإنها تدلّ على عدد الأجهزة المعرضة للخطر التي تتصل فِي وَقْتٍ وَاحِد بخادم القيادة والتحكم.

[2] عادة لا يتطابق عدد معين من عناوين بروتوكولات الإنترنت المحددة مع عدد الأجهزة، ويرجع ذلك إلى هناك عاملين يؤثران في الشبكة، أولهما: تحديد عناوين بروتكولات الإنترنت لنفس الجهاز على المدى القصير (بروتوكول تهيئة المضيف ديناميكيا "متأجج")، وثانيهما: مشاركة عدة أجهزة لعنوان برتوكولات إنترنت واحد (ترجمة عناوين الشبكة). فقد يكون عدد عناوين برتوكولات الإنترنت الفريدة أصغر أو أكبر من الأعداد المتَوَافِقة للأجهزة الفعلية، وهذا يتوقف على حجم بروتوكول تهيئة المضيف ديناميكيا وتأثيرات ترجمة عناوين الشبكة. ونظرا لارتفاع معدلات الاضطراب الذي يصاحب بروتوكول تهيئة المضيف ديناميكيا من قبل مقدمي خدمة الإنترنت التجارية، فإن أعداد العناوين الخاصة ببرتوكولات الإنترنت التي تم رصدها تعتبر عادة أكبر بكثير من عدد من الأجهزة

[3] فمن الأرجح أن عنوان برتوكولات الإنترنت تقوم علة قياسات فقط تتوافق جيدا مع عدد الأجهزة المصابة متى حدث ذلك على مدى فترات زمنية قصيرة، مثل ساعة واحدة. عناوين بروتكولات الإنترنت الفريد تم قياسها على مدى فترات زمنية أطول إلى حد كبير بسبب مرونة بروتوكول تهيئة المضيف ديناميكيا. في احدى الدراسات المعنية بشبكات الروبوت، وجد أن 1.25 مليون من عناوين برتوكولات الإنترنت الفريدة المصابة بفيروس الحواسيب المدمرة تم تحديدها في 10 أيام بالتطابق مع 183.000 فقط من شبكة الروبوت طبقا إلى لهوية الروبوت الفريدة. للمزيد، يرجى الاطلاع علي:
(Stone-Gross, B., et al. 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover. In: *16th Annual ACM Conference on Computer and Communications Security (CCS)*, 9-13 November 2009). In addition, zombie counts are affected by the 'no-see' time before a device or IP address is considered to no longer be a member of the botnet (see http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotCounts).

[4] أنظر على سبيل المثال:

http://www.secureworks.com/cyber-threat-intelligence/threats/waledac_kelihos_botnet_takeover/; http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/; Stone-Gross, B., et al. 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover. CCS '09.

بالإضافة إلى ذلك، فقد يوجد أيضا عدد أعلى بكثير من شبكات الروبوت الصغيرة، "الهواة"، تتألف من أعداد منخفضة من مجموعات الحواسيب المدمرة.[1]

الضَرَر – غير أن هذه الشبكات الخبيثة قادرة على إحداث ضرر جسيم؛ فخلال فترة عشرة أيام فقط، تم الكشف على أن أحد شبكات الروبوت المتصلة بحوالي 183,000 جهاز "زومبي" قد حصد ما يقرب من 310,000 من الحسابات المصرفية للضحايا، وبطاقات الائتمان، والبريد الإلكتروني، وتفاصيل مستخدمي الشبكات الاجتماعية.[2] وكما نوقش في القسم المعني "بمرتكبي الجريمة السيبرانية" في هذا الفصل، فإن إمْكانيّات شبكات الروبوت على حصد مثل هذه المعلومات ذات دور فعّال في تطوير الأفعال الإجرامية للجريمة السيبرانية، وذلك من خلال فتح "أسواق" تعتمد بشكل كبير على بيع شبكات الروبوت وتأجيرها.[3] وكما أفاد مكتب الأمم المتحدة المعني بالمخدرات والجريمة في تقييم خطر الجريمة المنظمة العابرة للحدود عام 2010، بأن سوق المعلومات الشخصية المتحصل عليها من خلال شبكات الروبوت يمكن تجزئتها إلى أجزاء فردية مختلفة تركز على جمع كميات من المعلومات المالية والمعلومات الخاصة بالهوية، وبيع هذه المعلومات وسحب المال بموجبها.[4]

أمثلة بشأن المعلومات المتحصل عليها من خلال شبكات الروبوت: "Torping"

- تخضع معرّفات القيادة والتحكم إلى رقابة باحثين أكاديميين لمدة 10 أيام
- تم تحديد عدد 183,000 جهاز "زومبي" خلال 10 أيام. متوسط أعداد أجهزة "الزومبي" النشطة في أي وقت 49,000. معظمها غالبا في شمال أوروبا وأمريكا الشمالية
- تم إرسال أوراق اعتماد حسابات 8,300 ضحية في 400 مؤسسة مالية مختلفة إلى خادم القيادة والتحكم
- تم إرسال تفاصيل 1,700 بطاقة ائتمان إلى خادم القيادة والتحكم
- تم إرسال 298,000 من أسماء مستخدمين وكلمات مرور لضحايا خاصة بالبريد الإلكتروني ومواقع التواصل الاجتماعي إلى خادم القيادة والتحكم
- عرض النطاق الترددي الكلي حَسْب حواسيب "الزومبي" لشن هجوم حجب الخدمة الموزعة

المصدر: Stone-Gross *et al*

[1] أنظر على سبيل المثال: http://www.symantec.com/connect/blogs/botnets-masses

[2] Stone-Gross, B., *et al.*, 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover. CCS '09

[3] أنظر على سبي المثال: Panda Security, 2010. *The Cybercrime Black Market: Uncovered.*

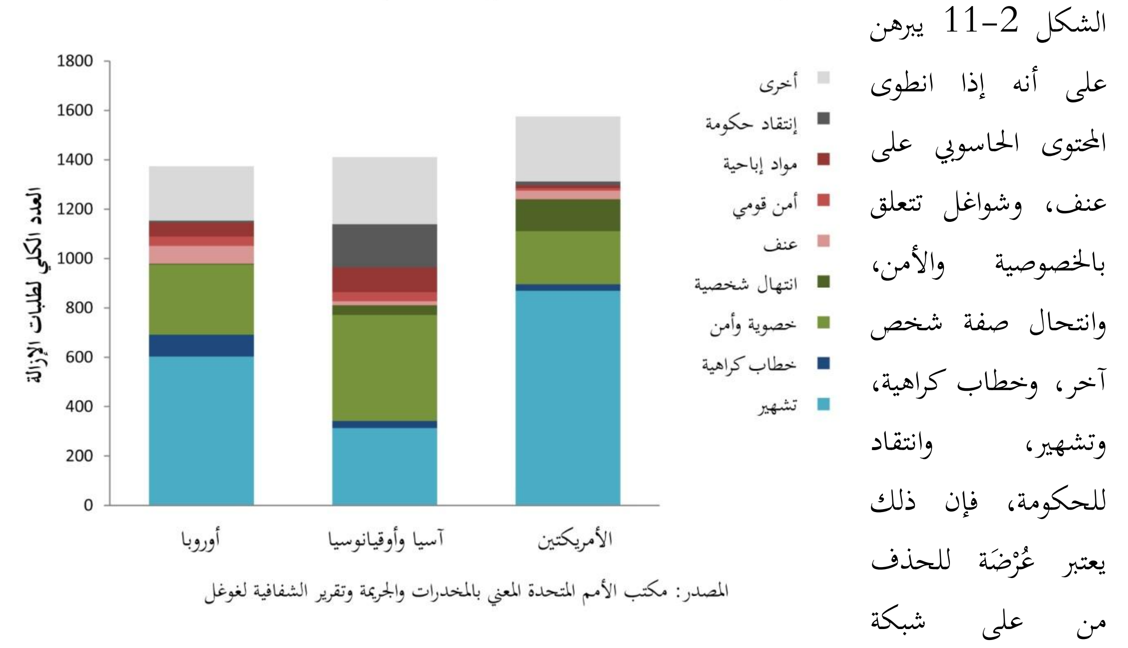
[4] مكتب الأمم المتحدة المعنى بالمخدرات والجريمة–تقييم خطر الجريمة المنظمة عبر الوطنية عام 2010

جرائم المحتوى

نظرة عامّة – يتعلق ما بين الثلث والنصف من الأفعال الشائعة التي تشكل الجريمة السيبرانية، بالمحتوى الحاسوبي.[1] ويضطلع القانون الجنائي بتنظيم محل الجريمة لعدة أسباب، منها؛ الأفعال التي تتعارض مع: الأمن القومي، أو السلامة العامة، أو النظام العام، أو الصحة والآداب العامة، أو حقوق وحريات الآخرين.

فعلى الصعيد العالمي، تشير المعلومات إلى أن خدمات جوجل تلقت أكثر من 4,600 طلب من قِبَل السلطات الوطنية لإزالة محتويات تتعلق بمجموعة واسعة من المواد قد اسْتَشَفّت الحكومات أنها تمس المجالات المذكورة أعلاه،[2] مع الأخذ في الاعتبار أن ليست كل هذه المواد ترتبط بشكل قاطع بالقانون الجنائي. وبالرغم من ذلك، فإن الشكل 2-11 يبرهن على أنه إذا انطوى المحتوى الحاسوبي على عنف، وشواغل تتعلق بالخصوصية والأمن، وانتحال صفة شخص آخر، وخطاب كراهية، وتشهير، وانتقاد للحكومة، فإن ذلك يعتبر عُرْضَة للحذف من على شبكة

الشكل 2-11: طلبات إزالة المحتوى التي تلقتها غوغل من حكومات 2010-2012



المصدر: مكتب الأمم المتحدة المعني بالمخدرات والجريمة وتقرير الشفافية لغوغل

الإنترنت. وتجدر الإشارة إلى أن العدد الإجمالي لطلبات الإزالة غير قابلة للمقارنة عبر مختلف المناطق، إلا أن أغلب طلبات الإزالة في جميع المناطق تنطوي على مواد تتعلق بالتشهير والخصوصية والأمن. وفي ضوء الاقتران بهذا النمط، فإنه أثناء جمع المعلومات الخاصة بهذه الدراسة، أشار عدد من البلدان في شمال أفريقيا وجنوب شرق آسيا إلى أن اتجاهات الجريمة السيبرانية يتمثل في: "*الازدياد المتواتر في استعمال شبكات التواصل الاجتماعي في التشهير بالآخرين، والدعاية*"، بالإضافة إلى "*الاتجاهات التصاعدية للأفعال المتعلقة بالسمعة والخصوصية*" و"*المنشورات التشهيرية عبر الإنترنت*".[3] وفي ضوء ما تمت مناقشته في الفصل الرابع (التجريم) في

---

[1] أنظر أعلاه، القسم 2-2: الصورة العالمية للجريمة السيبرانية، توزيع أفعال الجريمة السيبرانية.

[2] البيانات متاحة على: www.google.com/transparencyreport

[3] الاستبيان الخاص بالدراسة، السؤالان: 81 و58.

هذه الدراسة؛ فبينما من غير الممكن إطلاق حكم أخلاقي منفرد على المحتوى العالمي على الانترنت، إلا أن هناك مطالبة بوضع معايير صارمة متى استخدمت أدوات القانون الجنائي للحَدّ من حريات التعبير.[1]

استغلال الأطفال في المواد الإباحية – يجب أن تخضع المحتويات التي تتضمن مواد إباحية تستغل الأطفال إلى التدابير الجنائية، حيث اتضح خلال جمع المعلومات الخاصة بهذه الدراسة؛ أن الأفعال التي تنطوي على مواد إباحية عن الأطفال تشكل تقريبا ثلث الأفعال الأكثر شيوعا من الجرايمة السيبرانية التي تواجهها البلدان في أوروبا والأمريكتين، أما في آسيا وأوقيانوسيا؛ فكانت النسبة أقل، أي حوالي 15 في المائة.[2] فمنذ عام 2009، تم تحديد ما يقرب من 1,000 من المواقع الإلكتورنية التجارية التي تَفَرّدَت بنشر مواد إباحية عن الأطفال، ولكل موقع من هذه المواقع اسم مميز و"علامة تجارية" خاصة به، وكان نحو 440 موقعا من هذه المواقع نشطا خلال عام 2011،[3] حيث يعتبر كل موقع بمثابة بوابة لمئات أو آلاف الصور الفردية أو مقاطع الفيديو التي تظهر الاعتداء الجنسي على الطفل. وغالبا ما تُدعم هذه المواقع من قِبَل مستويات من آلية الدفع، أو محتويات مخزنة، أو نظم خاصة بالعضوية والإعلانات. أظهرت التطورات الأخيرة، ومنها عند التحميل المباشر من المواقع الإلكترونية يُعَرْض المحتوى القانوني، ولكن عند التحميل بطريقة معينة، فإن البوابة المخصصة للموقع تتيح الوصول إلى الصورة الإباحية للأطفال. بالإضافة إلى ذلك، فقد حددت إحدى العمليات التي تضطلع بها هيئات إنفاذ القانون، ضد تبادل الأقران لملفات تتضمن صورا إباحية للأطفال، عناوين برتوكولات الإنترنت الضالعة في تقديم ملايين من المواد الإباحية للأطفال.[4]

انتهاك حقوق الملكية الفكرية – حقوق الملكية الفكرية، هي مجموعة من الحقوق لحماية الإبداعات الفكرية للأشخاص، حيث تمنح هذه الحقوق للمبدع حقا حصريا لاستعمال مصنفاته لفترة معينة من الزمن. فكل المواد تقريبا التي تحميها هذه الحقوق يمكن أن تكون متاحة على شبكة الإنترنت، سواء كانت من المصنفات الأدبية أو الأعمال الفنية أو التسجيلات الصوتية، أو العلامات المميزة كالعلامات التجارية، وتفاصيل الاختراعات التي تحميها براءات الاختراع، أو الرسوم أو النماذج الصناعية أو الأسرار التجارية. ومتى انتهكت هذه الحقوق، عن طريق النسخ أو الاستعمال غير القانوني، فإن وسائل تطبيق القانون تكمن في رفع الدعاوى المدنية بين الأفراد، مع الاحتفاظ بحقهم في الادعاء المدني أمام المحاكم الجنائية في بعض الحالات. بالإضافة إلى ذلك، ففي بعض الحالات، قد ينعقد هذا الحق للدولة في اتخاذ الإجراءات الجنائية، فالاتفاقيات الدولية، بشكل عام، مثل اتفاقية تريبس (اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية)، تلزم الدول بفرض تطبيق العقوبات والإجراءات *الجنائية* على الأقل في حالات *"الانتهاك المتعمد وعلى نطاق تجاري."*[5]

---

[1] أُنظر الفصل الرابع (التجريم)، الجزء رقم 4-3 التجريم والقانون الدولي لحقوق الإنسان، القانون الدولي والقيود المفروضة على حرية التعبير.

[2] الاستبيان الخاص بالدراسة، السؤال رقم 81.

[3] مؤسسة الرقابة على الإنترنت 2011، التقرير السنوي لسنة 2011

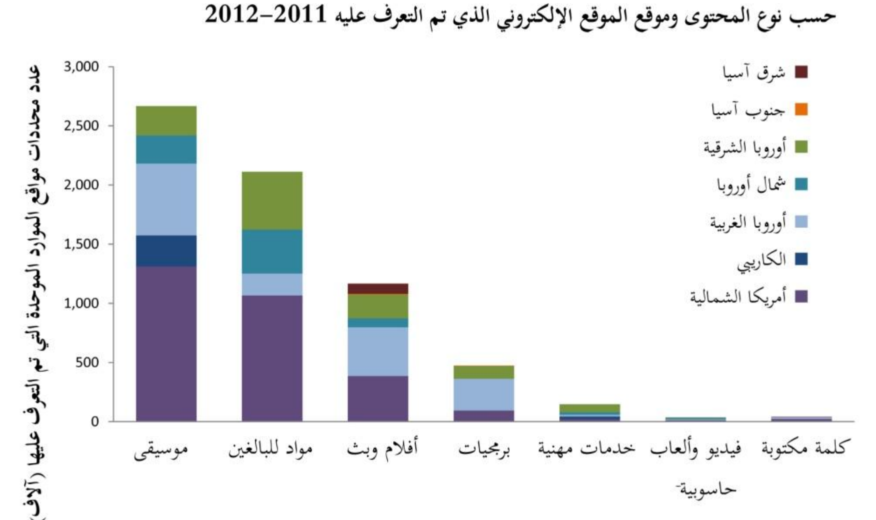
[4] اُنظر: http://www.justice.gov/psc/docs/natstrategyreport.pdf

[5] اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، المادة 61.

وفي ضوء ما تقدم؛ فإن تحديد طبيعة ونطاق أفعال التعدي الجنائي باستعمال الحاسوب على حقوق الملكية الفكرية يُعدّ من الأمور الصعبة. ولكن أفضل ما يمكن القيام به – على نطاق عالمي – لمواجهة هذا الانتهاك أو التعدي، يتمثل في تحديد مقدار المادة المرجح انتهاك حقوق الملكية الفكرية المقررة لها، بالإضافة إلى ماهية نوع هذه المادة، بشكل عام، وهذا يعتمد على سياق وظروف – بما في ذلك النطاق أو القصد أو الغرض، والقانون الواجب التطبيق والاختصاص القضائي – دَرَجَة الاستخدام المخالف من قبل الأفراد المتورطين فيه، والذين قد يخضعون إلى عقوبات جنائية بعد ذلك.

حقوق النشر – يتمتع الحق في حماية الكتب، والملفات، والموسيقى، والأفلام، وبرامج الحاسوب بأهمية خاصة بالنسبة للمحتوى الحاسوبي. على الصعيد العالمي، تشير التقديرات إلى أن ما يقرب من 24 في المائة من حركة الإنترنت تتمثل في انتهاك حقوق التأليف والنشر.[1] ويتغير مستوى حركة الانتهاك وفقا لمكان الإنترنت، حيث يبلغ مداه في مجالات مثل مواقع تبادل الملفات بين النظراء، مواقع تحميل فيروس "عدوى انتزاع الفدية"، والتي تستخدم بشكل شائع لتوزيع الأفلام والحلقات التلفزيونية والموسيقية وبرمجيات وألعاب الحاسوب.[2] ويعطي تحليل طلبات تتعلق بأكثر من 6.5 مليون من محددات مواقع الموارد الموحدة (URLs) من قِبَل أصحاب حقوق التأليف والنشر لإزالة محتوى مخالف من خدمات جوجل فكرة عن توزيع نوع من المواد، ومكان استضافة الموقع الإلكتروني.[3] وتتبلور أغلب طلبات أصحاب حقوق التأليف والنشر في إزالة المؤلفات الموسيقية المعتدى عليها، وتليها المواد الخاصة بالبالغين، والأفلام، والبث الإذاعي، وبرمجيات الحاسوب. بيد أن هناك طلبات تتضمن إلى حدّ كبير عددا أقل من الأشكال الأخرى من المحتويات. وجدير بالذكر، أن معظم

الشكل 2–12: طلبات إزالة متعلقة بحقوق النشر تلقتها غوغل من أعلى 60 مالك لحقوق نشر، حسب نوع المحتوى وموقع الموقع الإلكتروني الذي تم التعرف عليه 2011–2012



المصدر: مكتب الأمم المتحدة المعني بالمخدرات والجريمة وتقرير الشفافية لغوغل

[1] Envisional، 2011. التقرير الفني بشأن تقديرات التعدي على استخدام شبكة الإنترنت. كانون الثاني/يناير 2011. تستبعد هذه التقديرات كافة المواد الإباحية، وحالات الانتهاك التي يعصب تميزها.

[2] المرجع السابق.

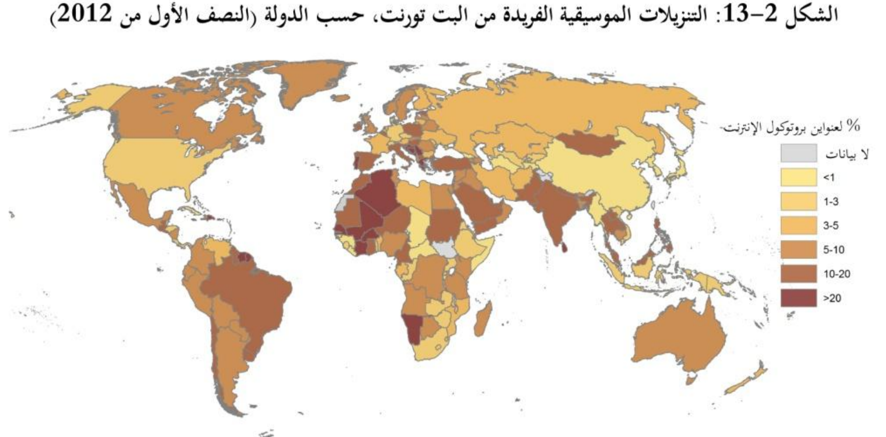
[3] وقد اقتصر التحليل على أعلى 60 طلب من أصحاب حقوق التأليف والنشر وفقا لعدد عناوين الموارد الموحدة المطلوب إزالتها. وقد أثرت النتائج الواردة من شركة جوجل بشأن طلبات الحذف على كل من طبيعة ونطاق المواد المخالفة واتجاه أصحاب الحقوق للبحث بنشاط عن المواد المعتدى عليها وطلب حذفها.

المواقع التي تستضيف هذه المواد تقع في أمريكا الشمالية وأوروبا، على الرغم من أن منطقة الكاريبي هي الأخرى تستضيف أيضا مواقع موسيقية مخالفة.

بينما لا يمكن استخدام هذه المعلومات للتَحَقّق من الانتهاك الجنائي لحقوق الملكية الفكرية، إلا أنه من الجدير بالملاحظة أن بعضا من طلبات الحذف الفردية المتعلقة بعدد من عناوين محددات مواقع الموارد الموحدة، والتي تصل أحيانا إلى عشرات الآلاف، قد تم تحديدها في مجال واحد.[1] في الواقع، لقد بدأ تحريك الدعاوى الجنائية ضد الأفراد المسؤولين عن استضافة مواقع إلكترونية تَتضَمَّن كمية كبيرة من المواد المخالفة ظاهريا والتي تتشابه مع المواد الأخرى المدرجة في بيانات طلب الإزالة المقدم إلى شركة جوجل.[2]

تظهر المعلومات العالمية المفصلة بشأن التنزيلات من أحد مواقع خدمة النظراء لتبادل الملفات، أو البت تورنت (ملف الرقم الثنائي) أن توزيع استخدام خدمات الإنترنت قد يمكن استخدامه في تبادل المواد المخالفة، حيث قُدرت قيمة إجمالي حركة البت تورنت بـ 18 في المائة من جميع حركة الإنترنت، ويشغل المحتوى الذي يتضمن مواد محفوظة الحقوق وغير إباحية ما يقرب من ثلثي هذه الحركة، مثل الأفلام والمسلسلات التلفزيونية والموسيقى وبرمجيات الحاسوب.[3]


الشكل 2–13: التنزيلات الموسيقية الفريدة من البت تورنت، حسب الدولة (النصف الأول من 2012)



المصدر: مكتب الأمم المتحدة المعني بالمخدرات والجريمة؛ Musicmetric Digital Music index

وتظهر الخريطة النسبة المئوية لإجمالي عناوين بروتوكولات الإنترنت حسب البلد، والتي تم تحديدها بشكل فريد والمتعلقة بتنزيل مواد موسيقية من البت تورنت، حيث تقدر بواحد من 750,000 من الفنانين المفضلين، وذلك في النصف الأول من عام 2012.[4] حيث تم تحميل بعض من المواد الموسيقية – بواسطة البت تورنت – التي أصْدرها هؤلاء الفنانون خلال هذه الفترة، وتقدر بـ 405 مليون إصدار موسيقي، أي ما يعادل تقريبا 80 في المائة من الألبومات الموسيقية، وأكثر بقليل من 20 في المائة من المقطوعات الموسيقية الفردية.[5] ويشير مُخَطّط التنزيل إلى ارتفاع

[1] أنظر: http://www.google.com/transparencyreport/removals/copyright/

[2] أنظر: http://www.justice.gov/opa/pr/2012/January/12-crm-074.html

[3] Envisional، 2011. التقرير الفني بشأن تقديرات التعدي على استخدام شبكة الإنترنت. كانون الثاني/يناير 2011.

[4] UNODC elaboration of data from MusicMetric. Digital Music Index. See www.musicmetric.com/dmi

[5] المرجع السابق.

نسبة التنزيل بصفة خاصة في بلدان أفريقيا وأمريكا الجنوبية وغرب وجنوب آسيا، وذلك بالنسبة إلى عدد عناوين برتوكولات الإنترنت في البلد.

قد لا يفي مثل هذا النشاط بوضع معايير نموذجية للتعدي الجنائي على حقوق الملكية الفكرية، ومع ذلك، أثناء جمع المعلومات الخاصة بهذه الدراسة، أشار عدد قليل من بلدان أمريكا الشمالية والجنوبية وأفريقيا إلى أن جرائم انتهاك حقوق التأليف والنشر وتقليد العلامات التجارية، باستخدام الحاسوب، شكلت مصدر قلق شائع بالنسبة للجريمة السيبرانية. وفي هذا الصدد، أشارت إحدى الدول في أفريقيا الجنوبية، على سبيل المثال، *"أن أحد أنواع أفعال الجريمة السيبرانية الأكثر شيوعا التي تشكل خطرا جسيما، يتمثل في إنتاج عمل فني غير قانوني، مما يؤدي إلى زيادة في البضائع المقلدة في السوق."* [1] ومع ذلك، قد أظهرت بشكل عام الردود الواردة على الاستبيان الملحق بهذه الدراسة، أن كيانات القطاع الخاص تعتبر جرائم انتهاك حقوق الملكية الفكرية ذات الصلة بالجريمة السيبرانية تهديدا أكبر من الجهود التي بذلتها الدول لمواجهة ذلك.[2] بيد أن ما يثير الاستغراب في هذا الصدد؛ أن استعمال الحاسوب في ارتكاب جرائم انتهاك حقوق التأليف والنشر وتقليد العلامات التجارية يعتبر للقطاع الخاص أقل بكثير من نطاق أفعال الجريمة السيبرانية الأخرى بشكل ملحوظ، مثل انتهاك الخصوصية أو انتهاك تدابير حماية البيانات أو اختراق النظام أو البيانات بصورة غير قانونية.[3]

3-2 مرتكبو الجريمة السيبرانية

الاستنتاجات الرئيسية

- لم يعد مرتكبو الجريمة السيبرانية بحاجة إلى مهارات أو تقنيات معقّدة، ويرجع ذلك إلى توافر الأدوات الخبيثة المجهزة والسريعة
- أكثر من 80 في المائة من أفعال الجريمة السيبرانية هي شكل من أشكال النشاط المنظم، حيث تقوم الأسواق السوداء للجريمة السيبرانية على دورة تتسم بإعداد البرمجيات الخبيثة والفيروسات الحاسوبية والتحكم بشبكات حاسوبية ("اعتداءات البوتنت") وتلقُّف البيانات الشخصية والمالية وبيع البيانات والمتاجرة بالمعلومات المالية
- غالبا ما تتطلب الجريمة السيبرانية درجة عالية من التنظيم – وقد تسْبَغ على نفسها صفة الجماعات الإجرامية الصغيرة – للاضطلاع بإدارة شبكات مخصصة طليقة أو ارتكاب جريمة منظمة على نطاق واسع، حيث تعكس النماذج الشخصية للجناة وأنشطة المجموعات الإجرامية في أكثر الأحيان أنماط من هذه النماذج المألوفة في العالم المادي

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 81.

[2] أنظر أعلاه، القسم 2-2 الصورة العالمية للجريمة السيبرانية، توزيع الأفعال التي تشكل الجريمة السيبرانية.

[3] المرجع السابق.

- ففي البلدان النامية بصورة خاصة، ظهرت شبكات فرعية تضم شبانا يرتكبون أعمال احتيال مالي بالحواسيب، بدأ كثيرون منهم بالتورط في الجريمة السيبرانية في أواخر سنوات المراهقة
- تعكس الطبيعة الديموغرافية للمجرمين الجريمة التقليدية حيث يشكل الشباب الذكور الأغلبية بين الجناة – بالرغم من أن التصنيف العمري يظهر تورط الأفراد من كبار السن (الذكور) – ولاسيما الجرائم المتعلقة باستغلال الأطفال في المواد الإباحية
- بينما أتم بعض الجناة مراحلهم في التعليم المتقدِّم، وبخاصة في مجال علوم الحاسوب، إلا أن العديد من المجرمين المعروفين لم ينالوا أي تعليم متخصص
- يوجد نقص في البحوث المنهجية حول طبيعة نشاط المنظمات الإجرامية في الفضاء الإلكتروني، حيث تبرز الحاجة إلى مزيد من الأبحاث التي تتعلق بماهية الروابط بين ارتكاب الجناة جرائم استغلال الأطفال في المواد الإباحية عبر الإنترنت وبدون الاتصال بالإنترنت

كما أوضحنا في القسم الخاص "بقياس الجريمة السيبرانية" في هذا الفصل، فإن توصيف الجريمة يتطلب بصفة عامة تحديد الجاني (وكم عدد الجناة) الضالع في ارتكاب الجريمة، وماهية الأفعال التي تشكل الجريمة المرتكبة وما مقدارها.[1] ويتناول هذا القسم، ماهية مقومات "الجاني"، مع التركيز على المسار النمطي للجناة وماهية المستويات المتوقعة لمنظمة إجرامية، مع الإشارة بصفة خاصة إلى جرائم الاحتيال الحاسوبي، وجرائم استعمال الحاسوب في انتاج أو توزيع أو حيازة مواد إباحية تستغل الأطفال.

وقد يتضمن الوَصْف الكامل "لمرتكب الجريمة السيبرانية" العديد من العناصر، حيث يعتبر العمر والجنس والخلفية الاجتماعية والاقتصادية والجنسية، ودوافع الجريمة من بين السمات الرئيسية للجاني.[2] بالإضافة إلى ذلك، فإن مستوى المنظمة الإجرامية يجَسّد الدرجة التي يتصرف بها الأفراد في التَنْسِيق مع الآخرين أو إحدى السمات المميزة للعنصر البشري الملازم للسلوك الإجرامي.[3] ويمثل استيعاب فكرة أن الجريمة السيبرانية تعتبر ظاهرة اجتماعية وتكنولوجية نهجا واسعا لمكافحة الجريمة، أكثر من ذلك الذي يرتكز فقط على المفاهيم التقنية للأمن السيبراني،[4] وذلك في ضوء تقييم سمات الأشخاص الذين يرتكبون مثل هذه الجرائم.

من المستقر أن تحديد السمات الفردية من الأمور البسيطة نسبيا، إلا أن تحليل الجريمة المنظمة كثيرا ما يبرز تحديات تتعلق بالقياس والتعريفات. وفي هذا الصدد، فإن هذه الدراسة تعتمد على المفهوم الواسع لماهية

---

[1] European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), 2011. Data Collection on [New] Forms and Manifestations of Crime. *In*: Joutsen, M. (ed.) *New Types of Crime, Proceedings of the International Seminar held in Connection with HEUNI's Thirtieth Anniversary*, 20 October 2011, Helsinki: EICPC. See also UNODC, 2010. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment.*

[2] إدارة الأمم المتحدة للشؤون الاقتصادية والاجتماعية، الشعبة الإحصائية 2003. دليل تطوير نظام إحصاءات العدالة الجنائية. الوثيقة رقم ST/ESA/STATSER.F/89

[3] أنظر: Levi, M., 1998. Perspectives on 'Organised Crime': An Overview. *The Howard Journal*, 37(4):335-345.

[4] أنظر: Yip, M., Shadbolt, N., Tiropanis, T. and Webber, C., 2012. *The Digital Underground Economy: A Social Network Approach to Understanding Cybercrime.* Paper presented at the *Digital Futures* conference, 23-25 October 2012, Aberdeen.

الجماعة الإجرامية المنظمة الوارد في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة.[1] ومن خلال هذا التعريف؛ توجد أساليب مختلفة للتصنيفات،[2] فضلا عن وجود أساليب لتصنيف جريمة جنائية ما "كجريمة منظمة".[3] وفي ضوء ذلك، لا يوجد أي سبب يدعو إلى الاعتقاد بأن تطور هذه التصنيفات والأساليب لا يمكن بطريقة أو بأخرى تطبيقه على تورط الجماعات الإجرامية المنظمة في ارتكاب الجريمة السيبرانية، ولو مع بعض التحديات الجديدة، وتحديديها على أساس كل حالة على حدة.[4] في الواقع؛ إن مفاد أحد الاقتِراحات الرئيسية الواردة في تقييم مكتب الشرطة الأوروبي (اليوروبول) بشأن التهديد الذي يشكّله تيسير شبكة الإنترنت للجريمة المنظمة يتمثل في أن "*هيكل جماعات الجريمة السيبرانية يشكل حتى الآن فجوة تعريفية واضحة من المفهوم التقليدي لجماعات الجريمة المنظمة باعتبارها مسألة متعلقة بالتسلسل الهرمي*".[5] وأخيرا، يوضح هذا القسم أنه بالرغم من أن هذا الأمر يعتبر حقيقيا في كثير من الحالات، إلا أنه من الضروري النظر في مجموعة واسعة من التصنيفات، بما في ذلك؛ الأخذ بعين الاعتبار ديناميكية النشاط الإجرامي عبر الإنترنت/ودون الاتصال بالإنترنت. في الواقع؛ إن مفاد أحد الاقتِراحات الرئيسية الواردة في تقييم مكتب الشرطة الأوروبي (اليوروبول) بشأن التهديد الذي يشكّله تيسير شبكة الإنترنت للجريمة المنظمة يتمثل في أن "*هيكل جماعات الجريمة السيبرانية يشكل حتى الآن فجوة تعريفية واضحة من المفهوم التقليدي لجماعات الجريمة المنظمة باعتبارها مسألة متعلقة بالتسلسل الهرمي*". وأخيرا، يوضح هذا القسم أن هذا الأمر، بالرغم من ذلك، يعتبر حقيقيا في كثير من الحالات، إلا أنه

---

[1] وفقا للمادة (2) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة، فإنه: يقصد بتعبير "جماعة إجرامية منظمة" جماعة ذات هيكل تنظيمي، مؤلفة من ثلاثة أشخاص أو أكثر، موجودة لفترة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الاتفاقية، من أجل الحصول، بشكل مباشر أو غير مباشر، على منفعة مالية أو منفعة مادية أخرى. وتنص الفقرة (ج) من المادة 2 على أنه: يقصد بتعبير "جماعة ذات هيكل تنظيمي" جماعة غير مشكلة عشوائيا لغرض الارتكاب الفوري لجرم ما، ولا يلزم أن تكون لأعضائها أدوار محددة رسميا، أو أن تستمر عضويتهم فيها أو أن تكون ذات هيكل تنظيمي".

[2] إحدى التصنيفات التي أوردها مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن الجماعات الإجرامية المنظمة تشتمل على: (أ) "المعيار الهرمي" (مجموعة هرمية فردية مع وجود أنظمة انْضِبَاط داخلية قوية)، (ب) "التسلسل الهرمي الإقليمي" (مجموعات مرتبة هرميا، مع وجود مَسَارات داخلية قوية من الرقابة والانضباط، ولكن باستقلال ذاتي نسبي للمقومات الإقليمية)، (ج) "تسلسل هرمي مُتَجَمِّع" (مجموعة من جماعات إجرامية أنشأت نظام تنسيق/رقابة–تتراوح بين القوة والضعف–على جميع أنشطتها)، (د) "المجموعة الرئيسية" (مجموعة منظمة بشكل محكم نسبيا، ولكنها مجموعة غير هيكلية، وتترك في بعض الحالات من قبل شبكة من الأفراد مُرْتَبِطة بأنشطة إجرامية)، و(هـ) "شبكة إجرامية" (وهي شبكة مرنة وطليقة، غالبا ما تتكون من أفراد ذوي مهارات خاصة، ويشكلون أنفسهم حول سلسلة مستمرة من المشروعات الإجرامية). مكتب الأمم المتحدة المعني بالمخدرات والجريمة 2002، نتائج الدراسة الاستقصائية التجريبية بشأن أربعين من الجماعات الإجرامية المنظمة المختارة في ستة عشر دولة. أيلول/سبتمبر 2002.

[3] لقد حدد مكتب الشرطة الأوروبي (اليوروبول)، على سبيل المثال، أنه لكي يتم تصنيف أي جريمة أو مجموعة إجرامية على أنها "جريمة منظمة"، يجب توافر ست خصائص على الأقل، أربعة منها يجب توافرها وهي الورادة في (1)، (3)، (5)، و(11)، وهي كما يلي: (1) أن يزيد عدد المشاركين عن فردين، (2) أن يكون لكل فرد مهمة محددة، (3) أن تكون مُتَمَدِّد لفترة من الوقت أو غير محددة المدة، (4) استخدام بعض من اشكال الانضباط والرقابة، (5) يشتبه في ارتكاب جرائم جنائية جسيمة، (6) تعمل على الصعيد الدولي، (7) تستعمل العنف أو الوسائل الأخرى المناسبة للترهيب، (8) استخدام هياكل تجارية أو نظامية، (9) أن يكون لها صلة بغسل الأموال، (10) ممارسة التأثير على السياسة والإعلام، والإدارة العامة، والسلطات القضائية أو الاقتصاد، (11) يحددها السعي وراء الربح و/أو السلطة. مكتب الشرطة الأوروبي (اليوروبول) وثيقة رقم 6204/2/97، ENFOPOL 35 Rev 2.

[4] على الرغم من ذلك، فعلى سبيل المثال، قد يكون المسؤول الفردي أو المؤسسي للكشف عن الحواسيب المعرضة لخطر شبكة الروبوت مساهم غير متعمد في عمل إجرامي، ذكر بعض المعلقين أن شبكة الروبوت يجب اعتبارها كشكل من أشكال الجريمة المنظمة Chang, L. Y. C., 2012. *Cybercrime in the Greater China Region*. Cheltenham: Edward Elgar).

[5] مكتب الشرطة الأوروبي (اليوروبول) 2011، تقييم بشان تهديد تيسير الإنترنت للجريمة المنظمة (الموجز)، ملف رقم 2530-264

من الضروري النظر في مجموعة واسعة من التصنيفات، بما في ذلك؛ الأخذ بعين الاعتبار ديناميكية النشاط الإجرامي عبر الإنترنت/ودون الاتصال بالإنترنت.

"الملامح النمطية" للجاني

لقد ساهمت الدراسات السابقة للمجموعات التي تمت محاكمتها في قضايا تتعلق بجرائم سيبرانية في توفير أغلب المعلومات الشائعة بشأن الملامح الفردية للجاني، كما تعتبر عمليات هيئات إنفاذ القانون السِرّيّة بشأن المنتديات الخَفِيّة على شبكة الإنترنت، فضلا عن رصد أعمال الجاني من قبل الباحثين الأكاديميين في الندوات النقاشية وغرف الدردشة، مصدرا قيما للمعلومات، كما توجد أساليب إضافية تساعد في جمع هذه المعلومات تتضمن استخدام استبيانات التقرير الذاتي (بدون ذكر أسماء)، ومراقبة مجريات الأنشطة "الأمنية السرية" حول تكنولوجيا المعلومات، وتطور تقنية الخوادم الخادعة "تقنية وعاء العسل" الموصولة بالإنترنت.[1] تعتبر الدراسات المقارنة من الأمور المعقدة، ويرجع ذلك إلى: الاختلافات في المنهجية المستخدمة، ومضامين وأفعال الجريمة السيبرانية، واختيار العينة، والتغطية الجغرافية، وأساليب تحليل

مشتبه فيهم بأفعال جريمة سيبرانية حدّدتهم الشرطة (دولة في جنوب آسيا)

في إحدى دول جنوب آسيا، نشرت الشرطة الوطنية إحصاءات تحتوي على تفاصيل تتعلق بجرائم سيبرانية مسجلة لديها. وقد تم تصنيف المشتبه فيهم في التقرير الإحصائي من خلال عدد من الفئات، طبقا للعلاقة بين المجني عليه والسمات الأخرى. بينما توجد نسبة عالية من المشتبه فيهم لم يتم تصنيفهم بعد، إلا أن إحصاءات الشرطة الوطنية تظهر التالي:

- يعتبر أكثر من 10 في المائة من المشتبه فيهم بارتكاب جريمة سيبرانية والمسجلين لدى الشرطة معروفين للمجني عليه، مثل الجيران والأصدقاء والأقارب،
- يشكل كل من الموظفين الساخطين وقراصنة الحواسيب نسبة 5 في المائة من مرتكبي الجريمة السيبرانية المسجلين لدى الشرطة،
- يعتبر عدد كبير من المشتبه فيهم بارتكاب جريمة سيبرانية مسجلين في التعليم العالي والبرامج التعليمية الأخرى.

المصدر: /http://ncrb.gov.in

استخدام الأعمال القانونية كسِتَار للجريمة السيبرانية

"يضطلع اثنان من المنظمين الأساسيين لإحدى المجموعات التي تتألف من حوالي 30 شخصا ومقرهما في أوروبا الشرقية، بتقديم خدمات الاستضافة والخوادم الحاسوبية القانونية. ومن خلال هذا النشاط المشروع، قاما بالتَسَتّر على المئات من "smswarez" (تجارة غير مشروعة في محتوى محمي بحقوق الطبع، مقابل الدفع من خلال خدمة الرسائل النصية القصيرة)، و"smswebs" (حيث يتم تنزيل صفحات من مواقع إلكترونية فيها محتوى محمي بحقوق الطب، مقابل الدفع من خلال خدمة الرسائل النصية القصيرة)، و"التورنت". واستخدم المنظمان رسائل البريد الإلكتروني الطفيلي (SPAM) للإعلان عن خدماتهم غير المشروعة، وهو ما أدى في النهاية إلى الحجز على 48 من الخوادم غير القانونية بسعة قدرها 200-250 تيرابايت. وبعد إلقاء القبض على هذه المجموعة، فقد انخفض مقدار حركة البيانات على الصعيد الوطني بنسبة 10 في المائة.

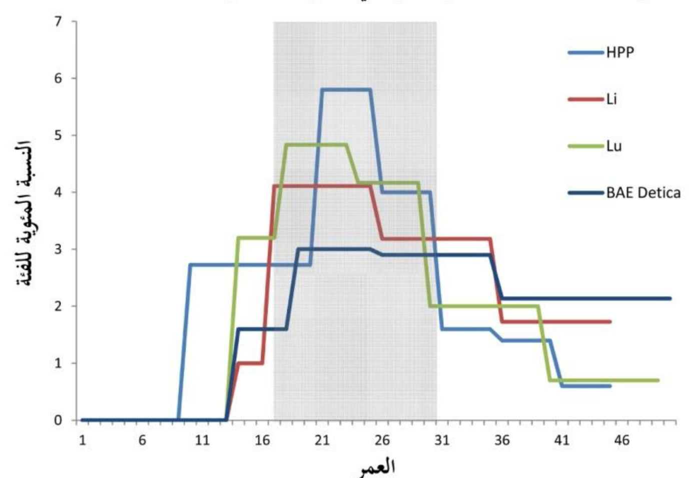
UNODC Digest of Organized Crime Cases

[1] أنظر على سبيل المثال: Chiesa, R., Ducci, S. and Ciappi, S., 2009. *Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking.* Boca Raton, FL: Taylor & Francis Group

وعرض سمات الجاني، مثل استخدام فترات عمرية مختلفة للجاني. ويتناول هذا القسم كل من البيانات المتعلقة بالدراسات المعنية بملامح مرتكبي الجريمة السيبرانية عبر مجموعة كبيرة من الجرائم، والبيانات التي تركز على أفعال مُعَيّنة؛ مثل: النفاذ غير المشروع لنظم حاسوبية أو اختراق البيانات الحاسوبية، وإنتاج أو توزيع أو حيازة المواد الإباحية المتعلقة بالأطفال بواسطة الحواسيب.

التحليل الوارد أدناه مَأخُوذ من ثلاث دراسات رئيسية[1] تتناول مجموعة كبيرة من أفعال الجريمة السيبرانية، فضلا عن دراسة استقصائية لتقرير ذاتي تركز على القراصنة.[2] وتتعلق الدراسة الأولى مجموعة "Li" التي تتكون من 151 من المجرمين الذين تمت مقاضاتهم جنائيا من قبل دولة في أمريكا الشمالية، عن قضايا "نمطية" من بالجريمة السيبرانية، في الفترة بين 1998 و2006.[3] أما مجموعة "Lu" تتألف من أكثر من 18,000 من المشتبه فيهم بارتكاب جريمة سيبرانية، مسجلين في قاعدة بيانات الشرطة في منطقة بشرق آسيا، بين عامي 1999 و2004.[4] وتناولت الدراسة، التي قامت بإعدادها شركة (BAE Detica)، عينتين من 250 من الأنشطة البارزة والمبلغ عنها لجماعات الجريمة "الرقمية" المنظمة، وذلك من خلال إحدى الرؤى التجريبية العالمية. وعلى النقيض من ذلك، فإن دراسة "HPP" المعنية بالقرصنة (مشروع القراصنة التوصيفي) تعتمد على بيانات واردة فيما يقرب من 1,400 استبيان تقرير ذاتي تم إكماله من قِبَل "القراصنة" – من الذين شاركوا (أو لم يشاركوا) في أي جريمة.[5]

الشكل 2–14: الفئات العمرية لمرتكبي الجريمة السيبرانية



المصدر: مكتب الأمم المتحدة المعني بالمخدرات والجريمة، HPP، Li، Lu، BAE Detica

---

[1] Li, X., 2008. The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted. *University of Ottawa Law & Technology Journal*, 5(1-2):125-140, ('Li'); Lu, C.C., Jen, W.Y., Chang, W. and Chou, S., 2006. Cybercrime & Cybercriminals. *Journal of Computers*, 1(6):1-10, ('Lu'); and BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age* ('BAE Detica').

[2] UNICRI and Chiesa, R., 2009. *Profiling Hackers*. Available at: http://www.unicri.it/emerging_crimes/cybercrime/cyber_crimes/docs/profiling-hackers_add-info.pdf ('HPP').

[3] وتضمنت مجموعة (لي) قرصنة/نفاذ غير مشروع، هجوم، التخريب، فيروسات، سرقة بيانات/تجسس، واستعمال الحاسوب في أعمال السرقة والاحتيال والاختلاس والفساد.

[4] وتضمنت مجموعة (و) الاحتيال عبر الإنترنت، القرصنة السيبرانية، سوء استخدام الحاسوب، واستعمال الحاسوب في غسل الأموال، المواد الإباحية، تجارة الجنس، المقامرة، وأعمال اللُصُوصِيّة.

[5] لاحظ المعلقون أن المفاهيم الثقافية الشائعة عن "القراصنة" غير محددة بشكل واضح، أو أن القراصنة بمثابة مرتكبي جرائم سيبرانية (ثغرات في المعلومات). أُنظر في هذا الصدد:

الفئة العمرية – يوضح الشكل 2-14 المجموعات العمرية لمرتكبي الجريمة السيبرانية من الدراسات الأربع،[1] حيث تظهر كل الدراسات أن أغلب الفئات العمرية من مرتكبي الجريمة السيبرانية تتراوح بين 18 و30 سنة. فمثلا، 27 في المائة من الجناة في مجموعة "Li" تتراوح أعمارهم بين 17 و25 سنة، أما مجموعة "Lu" فإن 53 في المائة من الجناة تتراوح أعمارهم بين 18 و29 سنة.

بيد أن الدراسة الحديثة التي أعدتها شركة BAE Detica تختلف إلى حد ما، حيث تشير إلى احتمالية ارتفاع مستويات استمرار ارتكاب الجرائم بين الأشخاص في الثلاثينات والأربعينات، تشير التقارير إلى أن 32 في المائة من الجناة تتراوح أعمارهم بين 36 و50 عاما. وعلى النقيض من الدراسات التي تشمل مجموعة من أفعال الجريمة السيبرانية، فإن الدراسة المعنية بالقرصنة (HPP) تظهر انخفاضا حادا في الفئات العمرية الأكبر سنا من الجناة، حيث تمثل الفئة العمرية 30 عاما نسبة 21 في المائة من كل مرتكبي الجرائم المذكورة أعلاه. وقد يعتبر ذلك مناسبا لتحديد الملامح الفرعية للقراصنة التي تبدأ في سن صغيرة، مثل الـ "script kiddies" (مصطلح لوصف من يعتمد على برمجيات وملفات مجهزة مسبقا للقيام بالقرصنة). وأخيرا، فإن الدراسة المعنية بالمشروع التوصيفي للقراصنة (HPP)، على سبيل المثال، تبين أن 61 في المائة من القراصنة، المشار إليهم في الدراسة، بدأوا في ممارسة القرصنة ما بين سن 10 و15 سنة. ومن ثم، فإن الفئة العمرية من إجْمالِيّ مرتكبي الجريمة السيبرانية أصغر من الضالعين في ارتكاب جرائم تقليدية بشكل عام. ففي منطقة شرق آسيا التي باشر فيها "Lu" ومجموعته أعمالهم الإجرامية، وجد أن قمّة الفئة العمرية لمجموع مرتكبي الجريمة تتراوح بين 30 إلى 39 عاما، مقارنة مع الفئة العمرية التي تتراوح بين 18 إلى 23 عاما من مرتكبي الجرايمة السيبرانية.

النوع الإجتماعي – يمثل الذكور الغالبية الساحقة من بين مرتكبي الجرايمة السيبرانية، حيث وجدت الدراسات المذكورة أعلاه (HPP, Li and Lu) أن 94 و98 و81 في المائة على التوالي من الجناة هم من الذكور. وتشير الحقائق إلى أن أكثر من 90 في المائة تتطابق مع نسبة الذكور المتورطين في الجريمة السيبرانية، وتشكل هذه النسبة درجة أعلى من الجريمة المعتادة، بشكل عام. فعلى الصعيد العالمي؛ يتراوح إجمالي نسبة الذكور الذين تمت محاكمتهم لارتكابهم أي جريمة ما بين 85 و90 في المائة، وبلغ المتوسط حوالي 89 في المائة.[2] يتناسب هذا النموذج مع البيانات التي قدمتها الدول أثناء جمع المعلومات الخاصة بهذه الدراسة. وقد علقت إحدى الدول في شمال أوروبا، على سبيل المثال، على أن *"الجناة هم من الشباب والذكور"*.[3]

Wall, D. 2012. The Social Construction of Hackers as Cybercriminals. *In:* Gregoriou, C. (ed), *Constructing Crime: Discourse and Cultural Representations of Crime and 'Deviance'.* Houndsmills, UK: Palgrave Macmillan, p.4-18.

[1] كما تفيد الدراسات بأن النتائج المترتبة على المخطّط تظهر أن أعمار الجناة ترتبط باستخدامهم في فترات عمرية مختلفة، وذلك وفقا لافتراض التوزيع المتساوي عبر فترات العمر المختلفة. وغالبا ما تظهر البيانات الأساسية لكل دراسة على حدة تَغَايُرا داخل كل فاصل زمني من العمر.

[2] مكتب الأمم المتحدة المعني بالمخدرات والجريمة والمعهد الأوروبي لمنع الجريمة ومكافحتها 2010. الإحصاءات الدولية بشأن الجريمة والعدالة. هلسنكي: معهد هلسنكي لمنع الجريمة ومكافحتها.

[3] الاستبيان الخاص بالدراسة، السؤال رقم 85.

ولقد تم إجراء عدد قليل من الدراسات في الدول النامية التي تقدم صورة واضحة تتناول كل الفئات العمرية. وبالرغم من ذلك، تؤكد الملامح الفرعية لمرتكبي الجريمة السيبرانية مثل جماعة (yahooboyes)[1] أن الشباب بصفة خاصة هم الفئة الأكبر، على الأقل، التي ترتكب أفعال الجريمة السيبرانية. وتشير إحدى هذه الدراسات القليلة إلى أن 50 في المائة من هؤلاء الجناة في إحدى دول غرب أفريقيا تتراوح أعمارهم بين 22 إلى 25 عاما، وقد إدعى أكثر من نصف هؤلاء أنهم قد قضوا بالفعل ما يقرب من خمس إلى سبع سنوات في الجرايمة السيبرانية.[2]

ملامح طلبة جماعة الـ (yahoobys) في إحدى دول غرب أفريقيا

العمر	
22 سنة فما دون	5 في المائة
22–25 سنة	50 في المائة
26–29 سنة	40 في المائة
29 سنة فما فوق	5 في المائة
الجنس	
ذكر	95 في المائة
أنثى	5 في المائة
عدد السنوات التي أمضيت في الجريمة السيبرانية	
2 سنوات فما دون	2.5 في المائة
2–4 سنوات	35 في المائة
5–7 سنوات	55 في المائة
7 سنوات فوق	7.5 في المائة
مستوى تعليم الوالدين	
بدون	2.5 في المائة
إبتدائي	5 في المائة
ثانوي	12.5 في المائة
ما بعد الثانوي	80 في المائة

Aransiola, J.O. and Asindemade, S.O. 2011.
Understanding Cybercrime Perpetrators and the Strategies they employ.
Cyberpsychology, Behaviour and Social Networking. 14(12), 759-763.

- *المهارات التقنية/الفنية* –

وفيما يتعلق بمستوى المهارة التقنية وإلْمام مرتكبي الجريمة السيبرانية بهذه المهارات، تشير الغالبية العظمى من الحالات التي تم تحليلها لمجموعة "Li" إلى أنها لم تنطوِ على مهارات أو تقنيات معقدة، شأنها في ذلك شأن القطاع الشائع من مستخدمي الحاسوب. وبصفة عامة، تتسم نسبة 65 في المائة من جميع الأعمال بالبساطة في تحقيقها، في حين تتطلب نسبة 13 في المائة مستوى من المهارات المتوسطة، أما النسبة الباقية (22 في المائة) تتطلب الإلمام بالمهارات التقنية بشكل دقيق للغاية.

كما أبرزت مؤسسات الأمن السيبراني بإيجاز؛ أن إمكانية شراء أدوات حاسوبية لديها قدرة على استغلال ثغرات الحاسوب والسيطرة على عدد كبير من الحواسيب؛ تعني أن مرتكبي الجريمة السيبرانية ليسوا في حاجة إلى

[1] تشير كلمة (*yahooboys*) إلى نمط من الشباب، ولاسيما الذين يعيشون في المدن، يقمون باستخدام الحاسوب في أعمال الاحتيال والتصيد ولنصب. للمزيد أنظر: Adeniran, A.I., 2011. Café Culture and Heresy of Yahooboyism. *In:* Jaishankar, K. (ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour.* Boca Raton, FL: CRC Press, Taylor & Francis Group.

[2] Aransiola, J.O., and Asindemade, S.O., 2011. Understanding Cybercrime Perpetrators and the Strategies they employ. *Cyberpsychology, Behaviour and Social Networking*, 14(12):759

مستويات عالية من المهارات التقنية،[1] ومن ثم، تعتبر مستويات المهارة التقنية على الأرجح مُتَغَيِّرَة بشكل كبير،[2] وكما هو مبين أدناه، فقد يؤدي ذلك في حد ذاته بعضا من الأدوار في هيكل مجموعة الجريمة السيبرانية. وعموما، ومن ناحية ثانية، فإن مستويات التعليم بين مرتكبي الجريمة السيبرانية تعتبر أعلى من مرتكبي الجرائم التقليدية، أو كل الجناة المتورطين في الجرائم التقليدية، حيث وجدت الدراسة التي كانت تتناول تحليل أنشطة مجموعة "Lu" أن نسبة 28 في المائة من المشتبه فيهم بارتكاب جريمة سيبرانية – في المجال محل الدراسة – قد تلقوا تعليما جامعيا، مقارنة مع 8 في المائة من الجناة المتورطين في جميع الجرائم. وعلى نحو مماثل، وجدت الدراسة المعنية بالقرصنة (مشروع القراصنة التوصيفي) أن أكثر من نصف عدد القراصنة قد تلقوا تعليما جامعيا. وبالرغم من ذلك، كما لاحظت الدراسة التي أعدتها شركة (BAE Detica) أنه من المرجح أن الاكتساب "الاصطناعي" للمهارات التقنية (وذلك من خلال الأدوات الخبيثة، ومنها ZeuS أو Butterfly Bot) قد أدى إلى التحول من الملامح التقليدية للمهارات العالية للإجرام الرقمي إلى تَجَمّع أوسع بكثير من الأفراد.

مرتكبو جرائم استغلال (تصوير) الأطفال في المواد الإباحية

قد تختلف ملامح مرتكبي جرائم استعمال الحاسوب في إنتاج أو توزيع أو حيازة مواد إباحية تستغل الأطفال، عن ملامح مرتكبي الجريمة السيبرانية بصفة عامة. ولقد قام "فريق العمل العالمي الافتراضي"،[3] بجمع معلومات حديثة بشأن مجموعة من الجناة الضالعين في هذه الجرائم من خلال عينة صغيرة غير عشوائية تتألف من 103 من الأشخاص الذين ألقي القبض عليهم على خلفية قيامهم بتحميل وتبادل مواد إباحية تستغل الأطفال عبر خدمة النظراء على الإنترنت.[4]

الفئة العمرية والحالة الاجتماعية – وفقا لفريق العمل العالمي الافتراضي، فإن الفئة العمرية لكل المشتبه فيهم كانت تتراوح بين ما بين 15 إلى 73 عام، بمتوسط فئة عمرية تبلغ 41 عام، كما أن واحدا من كل خمسة من المشتبه فيهم لا يعمل، فإما يكون متقاعدا أو عاطلا أو يتلقى إعانات اجتماعية تتعلق بالصحة. أما الآخرون فكان لديهم عمل أو يدرسون. حيث بلغت نسبة الذين يعيشون منهم مع شريك و/أو مع أطفال 42 في المائة. وهذه الفئة من الجناة تُعد من كبار السن بشكل ملحوظ (متوسط 50 عام)، كما أنها تشكل نسبة أكبر من الجناة الذين يعيشون بمفردهم، علاوة على ذلك، فإن كل المشتبه فيهم المعنيين كانوا يخفون

[1] See, for example, Symantec, 2011. *Report on Attack Kits and Malicious Websites*; Fortinet, 2013. *Fortinet 2013 Cybercrime Report – Cybercriminals Today Mirror Legitimate Business Processes*; and Trend Micro, 2012. *The Crimeware Evolution*

[2] وجد الدراسة المعنية بالقرصنة (HPP) على سبيل المثال: أن المهارات الفنية لدى القراصنة تعتبر كالتالي: مستوى منخفض (21 في المائة)، مستوى متوسط (32 في المائة)، مستوى عالي (22 في المائة) ، مستوى خبير متمرس (24 في المائة).

[3] فرقة العمل العالمية الافتراضية تعمل على مكافحة الاستغلال الجنسي للأطفال عبر الإنترنت، وأنشأت في عام 2003، وهي شراكة دولية بين ثمانية هيئات من هيئات إنفاذ القانون. أنظر: www.virtualglobaltaskforce.com

[4] لا تعتبر النتائج قابلة للتعميم على فئة المجرمين الضالعين في ارتكاب جرائم عبر الإنترنت، وذلك بسبب صغير العينة وعملية الاختيار غير العشوائية. ورغم ذلك، تم التعرف على بعض من السمات لهذه الأفراد ونشاطهم الإجرامي. أنظر:

Bouhours, B. and Broadhurst, R., 2011. *Statistical Report: Virtual Global Taskforce P2P Online Offender Sample July 2010–June 2011*. Canberra: Australian National University. Available at: SSRN: http://ssrn.com/abstract=2174815 or http://dx.doi.org/10.2139/ssrn.2174815

أنشطتهم عن الآخرين، ولكن نسبة 60 في المائة نجحوا في فصل أنشطتهم الإجرامية تماما عن حياتهم اليومية. أما الوضع بالنسبة لباقي المجموعة، فإن أنشطتهم الإجرامية ذات إفراط الى درجة غير سوية، كما كانت متشابكة مع حياتهم اليومية بشكل كبير أو قليل، علاوة على عدم إمكانية إخفائها بشكل جيد عن الآخرين. فهذه المجموعة تتميز بتدَهْوِرِ الوضع الاقتصادي والاجتماعي، مع ارتفاع نسبة الثقافة الحاسوبية، كما أن نسبة 4 في المائة منهم يعاني من مشكلة في الصحة العقلية.

النمط الإجرامي – توصف المدة الزمنية التي استغرقها المشتبه فيهم بارتكاب جرائم استغلال الأطفال في المواد الإباحية بأنها طويلة إلى حد ما، حيث تقدر بمتوسط خمس سنوات، وتتراوح ما بين ستة أشهر إلى 30 عاما. وتقوم نسبة 60 في المائة من المشتبه فيهم ليس فقط بتجميع المواد الإباحية عن الأطفال بل أيضا بالاتجار فيها أو توزيعها من خلال شبكة النظراء، كما أن نسبة 35 في المائة قد انخرطوا في شبكات أخرى بخلاف شبكات الأقران. بالإضافة إلى ذلك، فإن النصف من بين هؤلاء شاركوا في شبكات دون الاتصال بالإنترنت، مما يشير إلى أن الأفراد الذين يمارسون تجارة المواد الإباحية التي تستغل الأطفال عبر الإنترنت، يقومون بذلك أيضا بدون الاتصال بالإنترنت.

الروابط مع الأنشطة الإجرامية "دون الاتصال بالإنترنت" – للتمييز بين الجناة "عبر الإنترنت" والجناة "غير المتصلين بالإنترنت"، فإن الفئة الأولى تعتبر على الأرجح من الجنس القوقازي، عاطلون عن العمل، وأعمارهم بشكل هامشي أصغر من الفئة الثانية.[1] وبرغم من ذلك، قد توجد روابط بينهما.[2] وكشفت إحدى الدراسات الشارحة الحديثة أن واحدا من ستة من المجرمين متورطون في جرائم إستغلال أطفال في مواد إباحية دون الاتصال بالإنترنت، وذلك وفقا لإحدى العينات التي استندت إليها وشملت أكثر من 3,500 من مرتكبي جرائم استغلال الأطفال في المواد الإباحية عبر الإنترنت.[3] كما كشفت الدراسة التي اضطلعت بإعدادها فريق العمل العالمي الافتراضي، أن 6 في المائة من هؤلاء قد سبقت إدانتهم في جرائم جنسية ضد الأطفال عبر

[1] Babchishin, K., Hanson, R. and Herrmann, C., 2011. The Characteristics of Online Sex Offenders: A Meta-Analysis. *Sex Abuse: A Journal of Research and Treatment*, 23(1):92-123.

[2] See for example, Broadhurst, R. and Jayawardena, K., 2007. Online Social Networking and Paedophilia: An Experimental Research 'Sting.' *In:* Jaishankar, K., ed. *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, FL: CRC Press, 79-102; Elliot, A., Beech, A.R., Mandeville-Norden, R. and Hayes, E., 2009. Psychological Profiles of Internet Sexual Offenders: Comparisons with Contact Sexual Offenders. *Sex Abuse: A Journal of Research and Treatment*, 21(1):76-92; Endrass, J., Urbaniok, F., Hammermeister, L.C., Benz, C., Elbert, T., Laubacher, A. and Rossegger, A., 2009. The Consumption of Internet Child Pornography and Violent and Sex Offending. *BMC Psychiatry*, 9:43-49; Webb, L., Craissati, J., Keen, S., 2007. Characteristics of Internet Child Pornography Offenders: A Comparison with Child Molesters. *Sex Abuse: A Journal of Research and Treatment*, 19:449465.

[3] Wolak, J., Finkelhor, D., Mitchell, K., 2011. Child Pornography Possessors: Trends in Offender and Case Characteristics. *Sex Abuse: A Journal of Research and Treatment*, 23(1):22-42. دراسة أخرى تركز على مرتكبي جرائم استغلال الأطفال في المواد الإباحية، (دراسة بوتنر)، حيث قامت هذه الدراسة بإجراء مقارنة مجموعات من الجناة شاركوا في الفحص التطوعي، على أساس ما إذا كان لديهم توثيق تاريخي إضافي لمشاركتهم في جرائم جنسية على الأقل ضد أحد الأطفال. سلطت نتائج الدراسة الضوء على حقيقة أن العلاقة بين رؤية المواد الإباحية عن الأطفال والاتصال الجنسي المجرم يعتبر تفاعلا معقدا. فقد وجد أن الجناة عبر شبكة الإنترنت "لم يرتكبوا انتهاكات جنسية ضد طفل عبر الفعل المباشر بشكل ملحوظ"، وأن "العديد (منهم) تحرشوا جنسيا بالأطفال ولم يكتشف ذلك، وأن استخدامهم للمواد الإباحية عن الأطفال إنما يعبر عن نَزْعَة جنسية منحرفة. وإن لم يكن ذلك لأنشطتهم الإجرامية عبر الإنترنت، "فإن هؤلاء الجناة قد لا يثيروا انتباه هيئات إنفاذ القانون من نواح أخرى

الإنترنت، ونسبة 18 في المائة قد أدينوا بالاتصال مع طفل دون سن 16 عاما، علاوة على نسبة 15 في المائة أدينوا جرائم غير جنسية. بيد أنه يوجد تداخل قليل بين الأنشطة الإجرامية الجنسية وغير الجنسية، يتمثل ذلك في أن النزعة الإجرامية للمشتبه فيهم تنفرد في الإنتهاك الجنسي للأطفال. وكذلك وفي هذا الصدد؛ فإن المشتبه فيهم بالضلوع الراسخ في أنشطة استغلال الأطفال في المواد الإباحية عبر الإنترنت قد ارتكبوا، أو مازالوا يرتكبون، على الأرجح أيضا جرائم تتعلق بالاعتداء الجنسي على الطفل.[1]

وبصفة عامة، فالجناة في عينة فريق العمل العالمي الافتراضي لديهم معدل عالٍ نسبيا من الجرائم السابقة والمتزامنة مع أعمال إجرامية تتعلق بالاعتداء الجنسي على طفل دون الاتصال بالإنترنت. وفي الواقع، إذا كان أكثر من نصف المشتبه فيهم بارتكاب جرائم سابقة تتعلق بالاعتداء الجنسي على طفل، إلا أن هناك أدلة تشير أيضا إلى تورطهم الحالي في الاعتداء الجنسي على طفل. ونظرا إلى صغر حجم عينة فريق العمل العالمي الافتراضي واحتمالية التحيّز في الاختيار، فليس من الممكن الإجابة على السؤال بشأن ما إذا كان الرجال الذين تورطوا في جرائم استغلال طفل في مواد إباحية عبر الإنترنت يعتبرون أكثر عرضة للخطر من الذين تورطوا أيضا في أعمال إجرامية ضد الأطفال في "الحياة الحقيقة"، بيد أن هذا يمثل توجها هاما للبحث في المستقبل.

دور الجماعات الإجرامية المنظمة

تتطلب العديد من أفعال الجريمة السيبرانية درجة عالية من التنظيم والتخصص، فمن المرجح أن يكون مستوى ضلوع الجماعات الإجرامية المنظمة التقليدية في ارتكاب جريمة سيبرانية عالٍ، على الأقل في الجرائم السيبرانية التي تنطوي على دوافع مالية، مثل استخدام الحاسوب في الاحتيال والتزوير وجرائم الهوية. ومع ذلك، يجب التذكير، بأن تعريفات "الجريمة السيبرانية" و"الجريمة المنظمة" المعمول بها، ولاسيما توزيع أفعال الجريمة السيبرانية المختلفة

المقامرة عبر الإنترنت من قبل "عائلة" مافيا تقليدية

في عام 2008، قد وجه إلى 26 شخصا – بمن فيهم أعضاء "عائلة" مافيا للجريمة المنظمة المعروفة، في إحدى دول أمريكا الوسطى – تهمة فتح محل مُتَطَوّر بصورة غير شرعية، للمقامرة، بما في ذلك تشغيل أربعة مواقع إلكترونية للمقامرة. وقد علق المدعي العام للمقاطعة بالقول: "لقد أدت حملات إنفاذ القانون خلال السنوات الماضية بشأن إدارة عصابة إجرامية (المافيا) لصالات مراهنات تقليدية إلى زيادة استخدام عصابات القمار لمواقع إلكترونية للمقامرة تديرها مؤسسات خارجية بشكل غير قانوني، حيث يعتبر ذلك أمرا متاحا على مدار الساعة". وبينما اعتبرت المحاكمة في ظل الولاية القضائية الممنوحة لها أن المقامرة أمر غير قانوني، إلا أن المواقع الإلكترونية استغلت التشريعات المختلفة في ولايات قضائية أخرى. فالرهانات غير مجرّمة في الدولة، ولكن التجريم يتمثل في استغلال ذلك عبر مؤسسات خارجية وارتداد البيانات من خلال سلسلة من الخوادم المركزية للتَهَرّب من طرق الكشف التقليدية لإنفاذ القانون.

يرجى الاطلاع على:

http://www.fbi.gov/newyork/press-releases/2012/four-

[1] Bouhours, B., Broadhurst, R., 2011. *Statistical Report: Virtual Global Taskforce P2P Online Offender Sample July 2010–June 2011.* Canberra: Australian National University

ضمن أي فئة تناولتها، تؤثر في تقديرات "نسبة حالات الجريمة السيبرانية ذات الصلة بالجريمة المنظمة". فالأفعال التي تنطوي على استغلال الطفل في مواد إباحية، على سبيل المثال، قد تمثل مستوى أقل من "الجريمة المنظمة" إذا لم ينظر إليها الأشخاص الضالعون في تحميل هذه المواد الإباحية باعتبارها إجراء ضمن "هيكل الجماعة" لارتكاب إحدى الجرائم.

علاوة على ذلك، فإن تطبيق النماذج الحالية للجريمة المنظمة على الأنشطة الإجرامية "عبر الإنترنت" ليس بمنأى عن وجود تحديات لهذا التطبيق، حيث تعتبر السمات التقليدية للجريمة المنظمة مثل استخدام العنف والاستيلاء على الأراضي من الصعب الأخذ بها في توصيف النشاط الإجرامي السيبراني. بالإضافة إلى ذلك، لا تبدو المسائل المتعلقة بالمؤرُوث الإداري للجماعات الإجرامية المنظمة والتي تقوم على الثقة والتنفيذ، من الأمور اليسيرة التي تتوسط بيئة من مثل بيئة المنتديات عبر الإنترنت أو غرف الدردشة. وبالرغم من ذلك؛ ما يستطيع الأفراد فعله، يمكن للمنظمات أيضا فعله وربما بشكل أفضل. هذا، وتصلح شبكة الإنترنت والتكنولوجيات ذات الصلة بشكل جيد للتنسيق على نطاق أوسع بين الأفراد في منطقة جغرافية مترامية الأطراف، بما توفره من إمكانيات "لأسراب" الروابط الإجرامية قصيرة الأجل، وبين نماذج تقليدية متباينة، مثل المجموعات القائمة على التسلسل الهرمي والمعياري.[1] وكما هو مبين أدناه، فلقد تحوّلت الجريمة السيبرانية، في فترة زمنية قصيرة نسبيا، من انخفاض في حجم ارتكابها بواسطة فرد متخصص، إلى جريمة ذات حجم كبير وشائع و "بمثابة جريمة منظمة وصناعية".[2]

أوضحت إحدى الدراسات الحديثة، والتي أجرت استعراضا لعينة من 500 جريمة سيبرانية مسجلة لدى أجهزة الشرطة، أن ما يزيد عن 80 في المائة من الجريمة الرقمية تستلزم الآن بعضا من أشكال النشاط المنظم،[3] وقد تبلغ نسبة الجريمة المنظمة التي تنطوي على جريمة سيبرانية 90 في المائة، كتقدير أعلى.[4] ويزعم "تقييم خطر الجريمة المنظمة عبر الإنرنت – اليوروبول" (EUROPOL iOCTA) بأن الغالبية العظمى من التحقيقات في الجريمة المنظمة سوف تتطلب شكلا من أشكال التحقيق الخاص بالإنترنت في المستقبل القريب، في حالة عدم وجود فعلي لذلك. على الرغم من أن التقييم مُحَابٍ بشكل هادف لقضايا الجريمة المنظمة، إلا أن مكتب الأمم المتحدة المعني بالمخدرات والجريمة، في خلاصة لقضايا الجريمة المنظمة، انتهي إلى أن وجود جماعة إجرامية منظمة يعتبر عاملا متأصلا في جميع قضايا الجريمة السيبرانية التي تناولتها الخلاصة. حيث *"يجد بشكل كبير جدا دور القراصنة المنفردين باعتبارهم اللاعبين الأساسين في الجريمة السيبرانية"*.[5] وتشير الخلاصة أيضا إلى أن طبيعة الجريمة السيبرانية تتطلب *"بالضرورة تنظيم العديد من الوسائل والموارد البشرية"*.

---

[1] BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age*.
[2] Moore, T., Clayton, R., Anderson, R., 2009. The economics of online crime. *Journal of Economic perspectives*, 32(3):3-4
[3] BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age.*
[4] *Norton Cybercrime Report. 2011.* Available at: http://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf
[5] مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة في خلاصة لقضايا الجريمة المنظمة 2012، تجميع للحالات مع التعليقات والدروس المستفادة.

وفي هذا الصدد، ذكر أيضا عدد من الدول المجيبة على الاستبيان الخاص بهذه الدراسة أن هناك زيادة في تورط الجماعات الإجرامية المنظمة في الجريمة السيبرانية خلال السنوات الخمس الماضية. وأشارت، على سبيل المثال، إحدى دول غرب أفريقيا إلى *"تطور الجماعات الضالعة في ارتكاب الجريمة السيبرانية تعتبر أكثر تنظيما وتحقيقا لأهدافها في البعد العابر للحدود الوطنية*"، كما ذكرت إحدى الدول في أمريكا الجنوبية أن *"الجريمة السيبرانية انتقلت من كونها جريمة اقترفت من قبل مجرم منفرد إلى جريمة اقترفت من قبل منظمات إجرامية"*، كما خلصت إحدى دول جنوب شرق آسيا إلى أن *"الجريمة السيبرانية قد أصبحت واسعة الانتشار مع أداء كل فرد من الأفراد الدور المنوط به"*.[1]

ولذلك، يمكن اعتبار الجماعات الإجرامية المنظمة بمثابة *الجهات الفاعلة الأكبر في الجريمة السيبرانية*. ومع ذلك، فإن الأدلة التجريبية المحدودة تتطلب توخي الحذر، بخصوص الاستدلالات سواء فيما يتعلق بنسبة ضلوع الجريمة المنظمة وشكلها وهيكلها. فقد مَكّنت تكنولوجيا الحاسوب الأفراد أكثر من أي وقت مضى، حيث تشير واحدة من الدراسات حول الطلبة المشتبه فيهم بارتكاب جريمة سيبرانية، على سبيل المثال، إلى أن 77 في المائة منهم تصرّف بمفرده، وليس في مجموعة.[2] كما أفادت أيضا إحدى دول غرب آسيا المجيبة على الاستبيان؛ بأن معظم أفعال الجريمة السيبرانية *"اتخذت طابعا فرديا يُنفذه أناس لأغراض شخصية، وليست في شكل تنظيمات أو جماعات"*.

وكما ذكر أعلاه، فإن هذه الاستنتاجات قد تعتمد بشكل كبير على مفاهيم "الجريمة السيبرانية" المعمول بها، وطبيعة القضايا التي أثارت اهتمام السلطات الوطنية. وبصفة عامة تنتهج الجماعات الإجرامية في أغلب الأحيان أشكالا محددة من الجريمة السيبرانية، إلا أنه من الواضح أن كل التصنيفات، بما فيها الجناة من الأفراد، يجب أن تُؤخذ بعين الاعتبار. وتظهر القضية الواردة في الجدول، على سبيل المثال، إلى حد ما مجموعة من سمات الجناة من الأفراد والجماعات.

هيكل *الجماعة* – طرحت إحدى التحاليل الحديثة المعنية بالجريمة المنظمة والجريمة السيبرانية تصنيفا مبنيا على درجة تورط الجماعات الإجرامية المنظمة في ارتكاب جرائم عبر الإنترنت (مغاير لارتكاب الجرائم دون الاتصال بالإنترنت) وتَكْوين الروابط داخل الجماعة.[3] وفي هذا الصدد، تم وضع تصور يتمثل في تقسيم الجماعات الإجرامية إلى جماعتين؛ تضطلع الأولى بأنشطة واسعة تركز على البيئات الرقمية أو توجيه هذه الأنشطة نحوها، إضافة إلى ذلك، تُقسم إلى "أسراب" (التمحور على الإنترنت، هياكل معزولة) وموزعين

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 85.

[2] Lu, C.C., Jen, W.Y., Chang, W. and Chou, S., 2006. Cybercrime & Cybercriminals. *Journal of Computers*, 1(6):11-18.

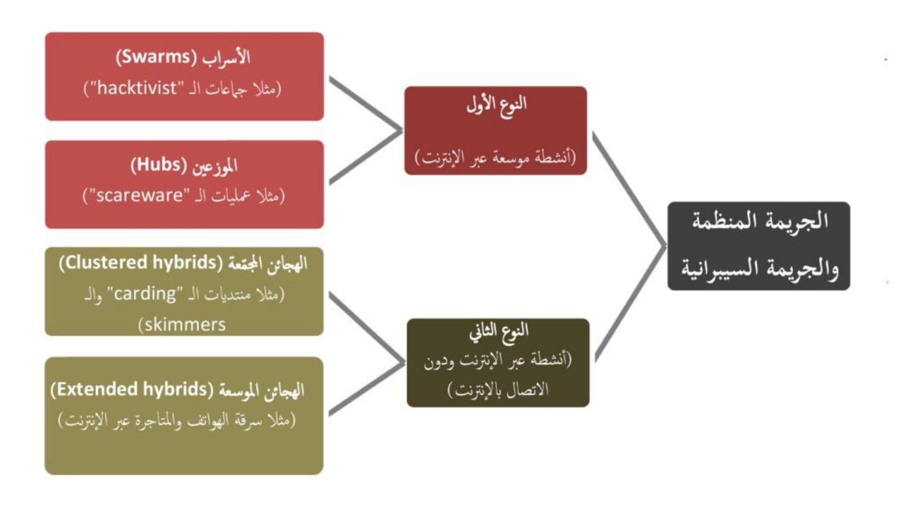
ووجدت الدراسة أيضا أن 63 في المائة من كل المشتبه فيهم بارتكاب جرائم سيبرانية تصرفوا باستقلالية. ومع ذلك، أشارت الدراسة إلى صعوبة كشف التواطئ، علاوة على أن الادعاء بارتكاب جرائم سيبرانية محددة بشكل مستقل، قد يخالف الواقع الذي أجاز ارتكابها في مجموعة.

[3] BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age.*

مركزيين (التمحور على الإنترنت، هياكل مرتبطة)، أما الثانية، فتباشر أنشطة تنتقل بين برامج على الإنترنت ودون الاتصال بالإنترنت، وعبرهما.

تضع الطبيعة الخلوية "للأسراب" وانحرافها عن المركز في ظل عدم وجود قيادة واضحة، عراقيل أمام حفظ الأمن والنظام العام، وذلك من خلال منظور إنفاذ القانون، ومن ناحية أخرى، هناك حقيقة مؤداها أن تلك الأسراب تُشكل غالبا من مجموعة "هواة"، وتتسم بضوابط ضعيفة بشأن "الالتحاق" بها، مما قد يتيح فرصا لحفظ الأمن والنظام العام. على النقيض من ذلك، توجد صعوبة بالغة في اختراق "الموزعين المركزيين"، بيد أن لديها هيكلا قياديا واضحا ونوافذ أساسية، تمكّن جهود هيئات إنفاذ القانون من مواجهتها. أما فيما يتعلق بالنمط الثاني من الجماعات الإجرامية؛ فلديها عمليات هجينة مُتَجَمِّعة وممتدة على هياكل مؤسسة على رابط متعدد، والتي يمكن من خلالها أن تكون هدفا لعمليات إنفاذ القانون المنفردة. فمن المستقر عليه؛ أن هذه الجماعات الإجرامية قد تكون مُنَسّقة بعض الشيء، ومع ذلك؛ توفر فرص لاتخاذ إجراءات تسلسلية ضد (من نواح أخرى) إحدى العمليات الإجرامية الفردية التي تضطلع بها.[1] علاوة على ذلك، فقد أدرجت فئة نمطية ثالثة من الجماعات الإجرامية تباشر أنشطة إجرامية دون الاتصال بالإنترنت بشكل أساسي، إلا أنها تتقاطع بشكل متزايد أو تقوم بوساطة عبر البيئات الرقمية.[2] وأخيرا، فمن الملاحظ أن الهياكل التنظيمية غالبا ما تتقاطع بطرائق عالية المرونة، غير أن الدلائل تشير إلى أن كافة هياكل هذه الجماعات تؤدي دورا في الأعمال الإجرامية السيبرانية، حيث من المرجح أن تصل نسبة هياكل الموزعين المركزيين والهجائن المجمعة ذات النطاق الواسع إلى 60 في المائة.[3]

الشكل 2–15: هياكل الجماعات الإجرامية المنظمة الضالعة في الجريمة السيبرانية



المصدر: BAE Detica/LMU

[1] المرجع السابق، صفحة رقم 51.
[2] المرجع السابق، صفحة رقم 52.
[3] المرجع السابق، صفحة رقم 60

أسواق الجريمة المنظمة والجريمة السيبرانية – لقد خضعت الهياكل التنظيمية للجرائم ذات الدافع المالي، مثل سرقة بيانات البطاقات المصرفية وبطاقات الإئتمان إلى تحليل خاصّ. ولقد حُدِّدت خصائص السوق السوداء للجريمة السيبرانية بجماعات وأفراد يؤدون في هذه الأسواق أدوارا مختلفة، وكثيرا ما تكون متعددة، (ففيهم "المبرمجون" و"الموزعون" و"الخبراء التقنيون" و"القراصنة" و"المحتالون" و"المستضيفون" و"الصرَّافون" و"نَقَلة الأموال" و"الزعماء")،[1] علاوة على أن هذه الجماعات والأفراد تتفاعل مع عدة عمليات منها إعداد البرمجيات الخبيثة، والتحكم في شبكات حاسوب مصابة (من خلال رسائل التصيد الاحتيالي)، وإدارة شبكات الروبوت، والحصول على البيانات الشخصية والمالية، والمتاجرة بالبيانات المالية.[2]

تفاعلات الجناة

تكشف الشكاوى التي حررتها سلطات إنفاذ القانون الجنائية في إحدى دول أمريكا الشمالية ضد مجموعة من مرتكبي الجريمة السيبرانية عبر الحدود الوطنية، وذلك في سياق الإجراءات، عن طبيعة تفاعلات الجناة داخل سوق الجريمة السيبرانية. الاقتباس التالي مقتطع من رسائل فورية أو "دردشات" تم الحصول عليها وفقا لسلسلة من أوامر التفتيش:

11:55:42:68 PM CC-4	كم سيكلفني برنامج تروجان (طروادة) الخاص بك؟
11:56:33:00:PM Alias-1	2ك في الشهر بما في ذلك الاستضافة والدعم
...	
11:56:55:38 PM Alias-1	يمكنك إعطاؤه (أي الوصول إلى الروبوت) لأناس مختلفين، الصراف وزملاء العمل
...	
12:28:22:32 AM Alias-1s	عندي امتداد ملف قابل للتنفيذ يعطي على الأقل من 200 إلى 300 دولارات من 1ك للتنزيل (للدول المختلفة) (أي الروبوت) سيوفر مبلغ 200 إلى 300 دولار أمريكي من العائدات المسروقة لكل 1,000 مجموعة من المعلومات المسروقة من الضحايا في (بلدان مختلفة)

المصدر: http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Kuzmin,%20Nikita%20Complaint.pdf

تعتبر المنتديات السرية أحد الأساليب التي تستخدمها الجماعات الإجرامية داخل السوق (المسيّرة غالبا بخدمات إخفاء الهوية أو "التسيير البصلي" مثل Tor لتبادل المعلومات والتوسط في بيع الخدمات الاستشارية، وخدمات الانتشار والفيروس، وتأجير شبكة الروبوت، وخدمات البريد الإلكتروني الطفيلي والاستضافة وقوائم البريد الإلكتروني والتفاصيل المالية.[3] ومن ناحية أخرى، فإن لمثل هذه الأسواق أن تضم عددا كبيرا من الأفراد، والمنظمات التي قد تكون عابرة، ولاسيما في حالة مهربي الأموال والأعمال والمعاملات التجارية المشبوهة مثل استئجار

[1] See http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom

[2] See, for example, Fortinet, 2013. *Fortinet 2013 Cybercrime Report*; Panda Security, 2010. The *Cybercrime Black Market: Uncovered*; and Group IB, 2011. *State and Trends of the Russian Digital Crime Market*

[3] See, for example, Motoyama, M. *et al.*, 2011. *An Analysis of Underground Forums*. IMC 2011, 2-4 November 2011, Berlin; and Stone-Gross, B. *et al.*, 2011. *The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns.*

الروبوتات من فرد واحد أو مجموعة إلى أخرى. هذا، وتستخدم شبكات الروبوت في ارتكاب الهجمات ضد نظم المعلومات وسرقة البيانات، وتُعرض بتكلفة منخفضة نسبيا، مستفيدة من تقلب حركة الأموال على أساس عدد العملاء. فعلى سبيل المثال، جهاز خادم مع برمجة خبيثة مخزنة عليه يشغل مجموعات أو مكونات شبكة روبوت يكلّف في أي مكان مبلغا قدره ما بين 80 إلى 200 دولارا أمريكيا في الشهر. مجموعة إدارة روبوت واحد، تعرف باسم مجموعة Eleonore Exploit Pack، تساوي في قيمة التجزئة مبلغ 1,000 دولار. أما استئجار شبكة روبوت ما بين 10 إلى 20 جهاز حاسوب تدار باستخدام هذه المجموعة فتبلغ تكلفته في المتوسط 40 دولارا في اليوم. أما عدة "زيوس" v1.3 فتبلغ تكلفتها من 3,000 إلى 4,000 آلاف دولار.[1] تعد هذه التكاليف منخفضة نسبيا بالمقارنة مع المكاسب المالية المحتملة التي قد تصل من عشرات الآلاف إلى عشرات الملايين من الدولارات.

وقد حُدِّدت خصائص سوق الجريمة السيبرانية بأنها "شبكات تواصل اجتماعي تتألف من أفراد ضالعين في نشاط إجرامي منظم"، وليست منشأة مؤلفة من جماعة إجرامية وحيدة.[2] وقد يمثل بعض الأفراد والمجموعات الصغيرة، مثل؛ المبرمجين الأصليين للبرمجيات الخبيثة وأصحاب شبكة روبوت قائمة على تكنولوجيا المعلومات، اللاعبين الأساسيين داخل السوق والذين يحوم حولهم تقريبا الأفراد الآخرون والأسراب، علاوة على الموزعين المركزيين. فمن الواضح أن هؤلاء الضالعين بإعداد وإدارة عناصر السوق الرئيسية، مثل شبكات الروبوت، يباشرون أفعالهم الإجرامية في شكل جماعات صغيرة نسبيا، أو حتى بشكل منفرد،[3] وذلك وفقا للتحقيقات التي أجرتها سلطات إنفاذ القانون وحالات القبض حتى هذا التاريخ. ويتضح من الدراسة التي أعدتها (BAE Detica/LMU)، بشأن المجموعات التي حددتها،[4] على سبيل المثال، أن أغلب النماذج التنظيمية الأكثر شيوعا تتألف من 3–5 أفراد قد عملوا سويا لما يقرب من سنة.[5] ووفقا لذلك؛ تتكون نصف المجموعات من 6 أفراد أو أكثر، ويضم الربع 11 فردا أو أكثر، حيث عملت ربع المجموعات النشطة لمدة أقل من ستة أشهر. وبالرغم من هذا لا يرتبط حجم المجموعة أو مدة تكوينها بمدى تأثير العمل الإجرامي، حيث يمكن للمجموعات الصغيرة إحداث ضرر جسيم خلال فترة قصيرة.

---

[1] ESET Latin America's Lab, 2010. *ESET, Trends for 2011: Botnets and Dynamic Malware.* Available at: http://go.eset.com/us/resources/white-papers/Trends-for-2011.pdf

[2] أنظر على سبيل المثال:

Spapens, T., 2010. Macro Networks, Collectives, and Business Processes: An Integrated Approach to Organized Crime. *European Journal of Crime, Criminal Law and Criminal Justice*, 18:285-215.

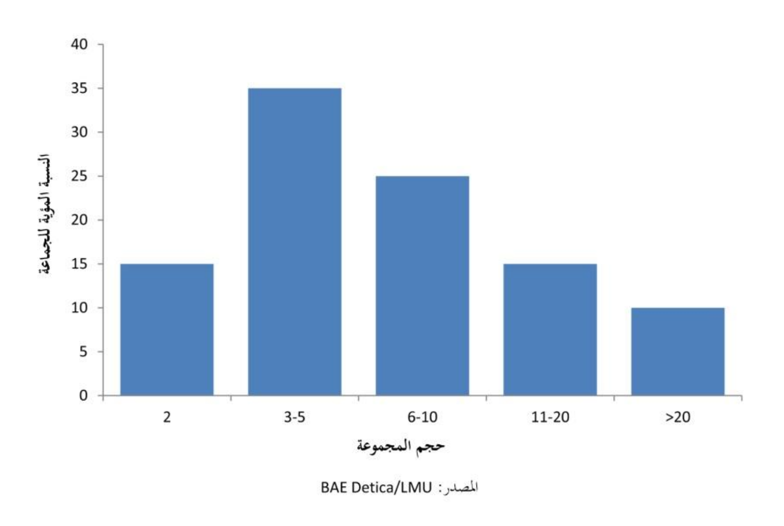
[3] See, for example, Bredolab botnet creator (http://nakedsecurity.sophos.com/2012/05/23/bredolab-jail-botnet/); Kelihos botnet creator (http://nakedsecurity.sophos.com/2012/01/24/microsoft-kelihos-botnet-suspect/); Mariposa botnet creator (http://nakedsecurity.sophos.com/2012/08/07/mariposa-botnet-trial/); and SpyEye convictions (http://nakedsecurity.sophos.com/2012/07/01/uk-cops-announce-sentencing-of-baltic-malware-trio/)

[4] وينبغي ملاحظة أن دراسة تشمل مجموعات من فردين. وتقع هذه الجماعات خارج نطاق التعريف المنصوص عليه في المادة رقم 2 من اتفاقية الجريمة المنظمة والتي تشير إلى مجموعة تتكون من ثلاثة أشخاص أو أكثر

[5] BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age*

وحيث إن الشروط القانونية لتعريف الجريمة المنظمة لا تسري على الأفراد والجماعات داخل سوق الجريمة السيبرانية، إلا أن من الممكن ضلوعهم في أعمال تتعلق بالمشاركة الجنائية أو الشروع بالاتفاق الجنائي، وذلك ضمن الأحكام الواردة في المادة 5 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة المعنية بالاتفاق الجنائي و/أو أنواع الجرائم التي تضطلع باقترافها الجماعات الإجرامية، فضلا عن المساهمة الجنائية المتمثلة في تنظيم أو توجيه أو مساعدة أو تحريض أو تيسير ارتكاب إحدى الجرائم الجسيمة التي تتورط فيها إحدى الجماعات الإجرامية المنظمة.[1]

الشكل 2-16: الأحجام النموذجية للجماعات الإجرامية المنظمة الضالعة في الجريمة السيبرانية



المصدر: BAE Detica/LMU

التوزيع الجغرافي – على الرغم من أن ثمة افتراض سائد يقضي بأن مجرمي الإنترنت يعملون بطريقة عالمية وغير مركزية إلا أن الدلائل تشير إلى أن تلك المجموعات ربما ما زالت محصورة في نطاقها الجغرافي حتى وإن كانت أنشطتها تتجاوز حدود الدولة. فعلى سبيل المثال، ما زالت الشبكات المحلية والإقليمية فضلا عن الشبكات القريبة من الأسرة والأصدقاء تعتبر من بين تلك العوامل الرئيسية. وفي الحقيقة، فإنه على الرغم من ارتباط تلك المجموعات بشكل كبير بالإنترنت، إلا أن ثمة دلائل على استخدامها أساليب

"البرمجية الخبيثة زيوس (ZeuS)"

استخدم أحد مهندسو برامج في أوروبا الشرقية برمجية خبيثة تعرف باسم "زيوس"، وبمجرد أن يفتح المجني عليه رسالة بريد الكتروني، يتم اختراق الحاسوب، وإن كانت الرسالة تبدو غير ضارة. ومن خلال الوصول إلى أرقام حسابات البنك الخاصة بالضحية وتفاصيل كلمة المرور، يستطيع المجرمون الدخول إلى حسابات البنك الخاصة به. ووضع المشاركون المسؤولون في الجريمة إشعارات على مواقع باللغة الروسية تدعو الطلاب القاطنين في أمريكا الشمالية للمساعدة في تحويل الأموال خارج البلاد. ويتم إمداد هؤلاء الذين يسموا "بناقلي الأموال" بجوازات سفر مزيفة وتم توجيهم لفتح حسابات بأسماء مزيفة في مختلف المؤسسات المالية في أمريكا الشمالية. وعندما يحول المسؤول الأموال من أصحاب الحسابات الشرعية إلى حسابات ناقلي الأموال، يتم إبلاغهم لنقل الأموال إلى حسابات خارجية أو في بعض الأحوال، لتهريب الأموال بأنفسهم خارج أمريكا الشمالية. وتم إلقاء القبض على خمسة أشخاص في أوروبا الشرقية و11 شخصا في شمال أوروبا وإدانة 37 شخصا في أمريكا الشمالية. ويبدو أن الدافع وراء المشاركين يتمثل بصورة رئيسية في إمدادهم بالمال. وقد جذبت الطبيعة المتكررة لجرائم الأفراد وحجمها اهتمام السلطات وساهمت في منع المؤامرات.

المصدر:

http://www.justice.gov/usao/nys/pressreleases/September10/operationachingmulespr%20FINAL

[1] أنظر اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة، فقرة (1/أ، ب)، المادة 5

تواصل وأنماط معرفة تحظى بسمات "محلية". وقد أدى هذا إلى حدوث تأثير محلي-عالمي تستخدم فيه جماعات إجرامية منظمة العوامل اللغوية لتعزيز أنشطتها. فعلى سبيل المثال، تتسم الكثير من المنتديات السرية عبر الإنترنت باستخدام اللغات المحلية وكذلك الأسماء المستعارة والعلامات الثقافية. ويكون لهذا تأثير على كل من صعوبة اختراق سلطات إنفاذ القانون وكذلك التحديد الذاتي لشركاء الجريمة الموثوق بهم.

تعتبر دول أوروبا الشرقية وشرق آسيا من الأماكن التي تشهد مستوى عال من نشاط الجريمة السيبرانية مع وجود صلات محتملة بالجريمة المنظمة. وعلى سبيل المثال، ظهرت برمجيات "زيوس" الخبيثة في أوروبا الشرقية عام 2007، وتم الإبلاغ عن موزعات (hubs) بارزة ضالعة في ارتكاب الجريمة السيبرانية في أماكن أخرى في أوروبا الشرقية.[1] ويتوافق هذا النموذج بشكل جيد ومثير للانتباه مع البيانات التي تحدد محل خوادم القيادة والسيطرة لشبكات الروبوت المشار إليها في هذا الفصل.[2] وأخيرا، فإن هناك قلق متزايد بشأن حجم الإيذاء السيبراني في شرق آسيا، بما في ذلك إمكانية وجود دور خطير لجماعات الجريمة المحلية.[3]

---

[1] Bhattacharjee, Y., 2011. Why Does A Remote Town In Romania Have So Many Cybercriminals? *Wired*, 19(2):82

[2] أنظر أعلاه، القسم -2، الصورة العالمية للجريمة السيبرانية، الأدوات الإجرامية -شبكة الروبوت

[3] Kshetri, N., 2013. *Cybercrime and Cybersecurity in the Global South*. Houndmills, UK: Palgrave Macmillan, Chapter 3; Broadhurst, R., Chang, Y.C., 2013. Cybercrime in Asia: trends and challenges. *In:* Hebenton, B., Shou, S.Y. and Liu, J. (eds.) *Asian Handbook of Criminology*. Springer

الفصل الثالث: التشريع وأطر العمل

يستهدف هذا الفصل دور التشريع الدولي والإقليمي والوطني، وأطر العمل، في منع ومكافحة الجريمة السيبرانية. ويبيّن أن التشريع مطلوب في كافة المجالات، بما فيها التجريم، ومنح الصلاحيات الإجرائية، والولاية القضائية، والتعاون الدولي. وفِيمَا قد شهد العقد الماضي تطورات هامة تتمثل في صدور صكوك متعددة الأطراف انْصَبّت على مكافحة الجريمة السيبرانية، فإن هذا الفصل يسلط الضوء على تجزؤ القانون بشكل متزايد، على الصعيدين الدولي والوطني.

1-3 مدخل - دور القانون

الاستنتاجات الرئيسية:

- يجب أن تنبري التشريعات أيضا للمفاهيم والموضوعات الجديدة، مثل عدم تصدي القانون لمسألة "بيانات الحاسوب" غير الملموسة، على النحو المعتاد، في ضوء التطورات التكنولوجية المرتبطة بالجريمة السيبرانية، في حين أنه من الممكن تطبيق القانون التقليدي إلى حد ما
- تعتبر التدابير القانونية من الأمور الأساسية لمنع الجريمة السيبرانية ومكافحتها، مما يتطلب أن تتناول هذه التدابير كافة المجالات المعنية بالتجريم ومنح الصلاحيات الإجرائية وتحديد الاختصاص القضائي والتعاون الدولي، بالإضافة إلى المسؤولية والتبعية التي يتحملها مقدم خدمة الإنترنت
- غالبا ما تُعنى قوانين مكافحة الجريمة السيبرانية بالتجريم، حيث تفرد جرائم مُخَصّصة للأفعال الرئيسية التي تشكل الجريمة السيبرانية، وذلك على الصعيد الوطني. ومع ذلك، أدركت الدول الحاجة الماسة لقوانين تتناول مجالات أخرى ذات صلة
- بالمقارنة مع القوانين السارية، فإن خطط وقوانين الجريمة السيبرانية الجديدة تتناول على نحو أكثر تواترا إجراءات التحقيق، والاختصاص القضائي، والأدلة الإلكترونية والتعاون الدولي

الخصوصية السيبرانية

تؤدي التدابير القانونية دور رئيسا في منع الجريمة السيبرانية ومكافحتها، حيث يعتبر القانون بمثابة أداة ديناميكية تُمكّن الدولة من التَجَاوُب مَع التحديات الاجتماعية والأمنية الحديثة، مثل تحقيق التوازن الملائم بين الخصوصية ومكافحة الجريمة، أو مدى مسؤولية الشركات التي تقدم خدمات الإنترنت. بالإضافة إلى القوانين

الوطنية، يتناول *قانون الأمم* – القانون الدولي – العلاقات بين الدول في كافة شؤونها التي لا حد لها، حيث تعتبر الأحكام الواردة في كل من القوانين الوطنية والقانون الدولي ذات صلة بالجريمة السيبرانية.

وفي هذا السياق، وفي ضوء التطورات التكنولوجية المرتبطة بالجريمة السيبرانية، فإنه يجب أن تتشابك التشريعات أيضا مع المفاهيم والموضوعات الجديدة، والتي لم يتناولها القانون بشكل مألوف. وجدير بالذكر، أن القوانين المتعلقة بالتطورات التقنية في العديد من الدول تعود إلى القرن التاسع عشر. بيد أن هذه القوانين لا تزال إلى حد كبير تركز على الموضوعات المادية التي تدور في فلك الحياة اليومية للمجتمع الصناعي، ولهذا السبب، لا تأخذ العديد من القوانين العامة التقليدية بعين الاعتبار خصوصيات المعلومات وتكنولوجيا المعلومات التي ترتبط مع الجريمة السيبرانية، والجرائم التي تتمخض عن ارتكابها أدلة إلكترونية، حيث إن هذه الأفعال متسمة بموضوعات *معنوية* جديدة، مثل البيانات أو المعلومات.

ولئن كانت *الموضوعات المادية* يمكن أن تنسب عادة إلى مُلاك محددين بشكل حصري، إلا أن إسناد ملكية *المعلومات* قد يؤدي بشكل ملحوظ إلى مزيد من التحدي. ويعتبر هذا التباين ذا صلة بالمفهوم القانوني "للسرقة"، على سبيل المثال، المعمول به في القانون التقليدي للعديد من الدول، إلا أن "سرقة" بيانات حاسوبية، على سبيل المثال، قد يستبعد من نطاق العناصر التي تقوم عليها جريمة السرقة التقليدية، حتى في ضوء تمديد نطاق الموضوعات التي تشتمل على البيانات أو المعلومات. وبالتالي؛ ستبقى البيانات في حيازة الحائِز الأصلي، حيث من المحتمل (اعتمادا على النهُج التي يقوم عليها القانون الوطني) ألا تستوفي العناصر المطلوبة لقيام الجريمة، مثل "نزع الملكية" أو "الاستيلاء على الملكية". وعلى نحو مماثل، (ومرة أخرى، اعتمادا على النهج التي يقوم عليها القانون الوطني) فقد يجوز أو لا يجوز تمديد نطاق المرجعية القانونية لمكان عام أو خاص في قوانين التحرش أو الملاحقة، لتشمل "الأماكن" عبر الإنترنت. فهذه الأمثلة تستجلي حاجة مُحْتَمَلة، في بعض المجالات، لمِسَايَرَة القواعد القانونية لتكنولوجيات المعلومات الجديدة.[1]

وظائف تشريعات الجريمة السيبرانية

- وضع معايير سلوكية واضحة لاستخدام أجهزة الحاسوب.
- رَدْع الجناة وحماية المواطنين.
- تمكين سلطات إنفاذ القانون من إجراء التحقيقات مع حماية الخصوصية الفردية.
- توفير إجراءات عادلة ومنصفة للعدالة الجنائية.
- الإلزام بالحد الأدنى من معايير الحماية في مجالات مثل التصرف في البيانات والتحفظ عليها.
- تمكين التعاون بين الدول في المسائل الجنائية التي تنطوي على جرائم سيبرانية والأدلة الإلكترونية.

وهذا يثير تساؤلا بشأن ما إذا كان يجب أن تتناول الأحكام العامة للقانون الجنائي الساري الجريمة السيبرانية، أم ينبغي وجود تشريعات جديدة تتصدى لها أو تقنن أحكاما خاصة بالجرائم الحاسوبية. بيد أنه بشكل عام، لا يمكن الإجابة على هذا السؤال،

[1] Sieber, U., 2012. Straftaten und Strafverfolgung im Internet. *In*: *Gutachten des Deutschen Juristentags*, Munich: C.H. Beck, pp.C 14-15

ولكن بالأحرى يعتمد على طبيعة الأعمال الفردية ونطاق القوانين الوطنية وتفسيرها. ويتناول الفصل الرابع (التجريم) من هذه الدراسة استخدام القوانين العامة والتخصصية في تجريم الأفعال التي تشكل الجريمة السيبرانية. وتوضح ردود الدول على الاستبيان الخاص بهذه الدراسة أن بعضا من أفعال الجريمة السيبرانية "الأساسية" قد أُدرجت ضمن أفعال جريمة سيبرانية محددة، في حين استوعبت الجرائم العامة أفعال الجريمة السيبرانية الأخرى.[1] أما الفصل الخامس (إنفاذ القانون والتحقيقات) والفصل الثامن (المنع) فيعتبران أن استعمال قوانين خاصة بالمعلومات أو بالجريمة السيبرانية من الأمور المطلوبة في مجالات مثل؛ منح صلاحيات لسلطات إنفاذ القانون عند إجراء التحقيق[2] وتحديد ماهية مسؤولية موزعي خدمة الإنترنت.[3]

فئات القانون ذات الصلة

لما كان يُنظر إلى القانون الجنائي باعتباره الأكثر ملائمة متى تعلق الأمر بجريمة سيبرانية، فإن ردود الفعل القانونية الممكنة تدعو أيضا إلى مراعاة القانون المدني (الذي يضطلع بتنظيم العلاقة القانونية بين الأشخاص)، والقانون الإداري (الذي يضطلع بتنظيم العلاقة القانونية بين الدولة والأفراد)، بالإضافة إلى الأقسام الأخرى في هذه النظم القانونية، ومنها القوانين الإجرائية والقوانين الموضوعية، إلى جانب ذلك، القوانين التنظيمية والدستورية، أو القوانين القائمة على الحقوق. ويختص كل نظام على حدة، في العديد من النظم القانونية، بأهداف ومؤسسات وضمانات محددة، حيث عادة ما توجد قوانين مكافحة الجريمة السيبرانية ضمن مجالات قانون الإجراءات الجنائية والقوانين الموضوعية، إلى جانب عدد من المجالات الأخرى للقانون تعتبر أيضا هامة.

وبصفة خاصة، لا تتطلب دائما مجموعة الأفعال التي تشكل جرائم ذات صلة بالحاسوب والتي تأمل الدولة في تنظيمها تغليب تدابير جنائية متداخلة، حيث يمكن أن يتصدى القانون الإداري والقانون المدني، على سبيل المثال، للأفعال ذات الصلة بالحاسوب التي تعتبر انتهاكات بسيطة، بدلا من القانون الجنائي. بالإضافة إلى ذلك، تشير غالبا القوانين الجنائية إلى المعايير الأساسية للقانون المدني والقانون الإداري، مثل مجالات قانون حقوق التأليف والنشر أو قانون حماية البيانات، مما يتطلب أيضا وجود أحكام مُتَآلِفة تجمع بين المسؤولية الجنائية والإدارية والمدنية في آن واحد. وبالتالي؛ يجوز أن يتناول التشريع المعني بالجريمة السيبرانية مجموعة كبيرة من الأمور، منها: تجريم سلوك معين، والصلاحيات الممنوحة للشرطة في جمع الاستدلالات، والمسائل التي تتعلق بالاختصاص

---

[1] أُنظر الفصل الرابع (التجريم)، القسم 1-4 لمحة عامة عن التجريم، الجرائم السيبرانية الخاصة والجرائم العامة.

[2] تطرح الدراسات الحالية فكرة أن أحكام خاصة تتعلق بالحاسوب، أمر مطلوب في صلاحيات التحقيق ليجيز اتخاذ ما يلزم من الإجراءات مثل، اصدار أمر معجل بالتحفظ على البيانات واستخدام أدوات الطب الشرعي عن بعد. للمزيد أُنظر:

Sieber, U., 2012. Straftaten und Strafverfolgung im Internet, *In: Gutachten des Deutschen Juristentags*. Munich: C.H. Beck, pp.C 62-72, 103-128

[3] نقل أو استضافة أحجام كبيرة من محتويات الغير من قبل مقدمي خدمات الإنترنت، على سبيل المثال، جعل قواعد المسؤولية التقليدية للتطبيقات المتعذر تنفيذها تسري على الصحافة ووسائل الإعلام، والذي يلتزم غالبا برقابة المحتوى قبل النشر. وبالأحرى، تعتبر المسؤولية العامة قد استبدلت بموجب شروط خاصة، منها الإجراءات المتعلقة بـ "الإخطار" و"التسجيل". أُنظر الفصل الثامن (المنع)، القسم 3-8، مكافحة الجريمة السيبرانية، القطاع الخاص، والمؤسسات الأكاديمية، ومكافحة الجريمة السيبرانية من قبل مقدمي خدمات الإنترنت والاستضافة.

القضائي الجنائي، وقبول الأدلة الإلكترونية، ومسؤوليات مقدمي الخدمات الإلكترونية لحماية البيانات، وآليات التعاون الدولي في المسائل الجنائية التي تنطوي على جريمة سيبرانية.

وقد عكست ردود الدول على الاستبيان الخاص بهذه الدراسة اتساع هذه المجالات، حيث أشارت عندما سُئلت عن ماهية القوانين ذات الصلة بالجريمة السيبرانية، إلى عدد من القوانين، منها القوانين الجنائية، وقوانين جرائم التكنولوجيا العالية، وقوانين الإجراءات الجنائية، والقوانين المتعلقة بالتصنت على المكالمات الهاتفية، وقوانين الإثبات، والقوانين المتعلقة بالاتصالات الإلكترونية، وقوانين المعاملات الإلكترونية، وقوانين الأمن السيبراني، وأخيرا القوانين المتعلقة بالتعاون الدولي.[1]

يظهر الشكل 3-1 المجالات التي تناولتها التشريعات حسبما أبلغت الدول من خلال الدراسة الاستقصائية، كما توضح البيانات عملية توزيع أكثر من 250 تشريعا قائما، وأكثر من 100 جزء من أجزاء التشريع الجديد أو المخطط لذلك.[2] ويعتبر التجريم بمثابة المجال الأقوى الذي تركز عليه كل من القوانين أو الخطط سواء القائمة أو الجديدة. وعلى النحو المبين في الفصل الرابع (التجريم)، فإن ذلك يتضمن كلا من الأحكام الجنائية العامة والخاصة ذات الصلة بالجريمة السيبرانية. وغني عن البيان، فإن التجريم يقدم أكثر المجالات المعتادة للقوانين أو التشريعات الجديدة، حيث تشير الدول باستمرار إلى التركيز على تقنين جرائم سيبرانية جديدة ومحددة، و/أو التكيف مع الجرائم العامة المنصوص عليها، أو العمل على تعديلها.

الشكل 3-1: مجالات التشريع المعنية بالجريمة السيبرانية

	التشريعات القائمة	تشريعات جديدة أو مخطط لها
التجريم	38%	27%
إجراءات التحقيق	15%	17%
الولاية القضائية	11%	14%
الأدلة الإلكترونية	9%	13%
التعاون الدولي	6%	12%
المنع	9%	6%
التعاون العام–الخاص	5%	5%
أخرى	6%	5%

المصدر: إستبيان دراسة الجريمة السيبرانية. السؤال 12 و14. (رقم 36،55؛ 111،262)

ويلاحظ أن تخفيض حَجْم التشريعات أو المخططات الجديدة بشكل نِسْبِيّ (مقارنة مع التشريعات القائمة) التي تتعلق بالتجريم، وزيادة الاهتمام النسبي بالمجالات الأخرى، مثل إجراءات التحقيق، والولاية القضائية، والأدلة الإلكترونية، وعلى وجه الخصوص التعاون الدولي يستجلي رَغْبَة في تعزيز الاعتراف بالحاجة إلى تشريعات

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 12.

[2] الاستبيان الخاص بالدراسة (الردود بشأن التشريعات)، السؤال رقم 12، و14.

تتعلق بمكافحة الجريمة السيبرانية عبر مجموعة من المجالات التشريعية، وهذا على الأقل ما عبرت عنه البلدان المجيبة على الاستبيان الخاص بالدراسة.

من قبيل طرح هذه المجالات التشريعية، يقّدم هذا القسم بإيجاز الاعتبارات القانونية ذات الصلة لكل منها.

التجريم – من المقرر قانونا، من ناحية، أن مبدأ *لا جريمة إلا بنص* (لا جريمة بدون قانون) يتطلب أن يكون الفعل مناط التجريم منصوصا عليه بوضوح في القانون.[1] وكما تم تناوله أعلاه؛ فقد تتطلب القوانين الجنائية مدخلا للمعلومات الجديدة ذات الصلة بالأغراض القانونية، فضلا عن تمديد الحماية القانونية التقليدية للمصالح ضد الأنماط الجديدة من الأفعال الإجرامية ذات الصلة بالحاسوب، وذلك من أجل إعطاء وصف للفعل الذي يشكل الجريمة السيبرانية بشكل واضح. ومن ناحية أخرى، فإن الأهداف الجديدة قد تطالب بإدراج تعريفات، مثل "ماهية البيانات الحاسوبية" أو "المعلومات الحاسوبية، ومصالح القانونية مثل "سلامة" نظم الحاسوب.

من خلال هذه المفاهيم، فإن القانون الجنائي يمتلك من الأدوات ما يكفل حماية المصالح "السيبرانية" – التي تعود للأشخاص – ضد الانتهاكات، مثل التحكم في الوصول إلى نظم الحاسوب التي يمتلكونها. فمن الثابت، أن لدى الأنظمة القانونية المختلفة معايير أساسية لتحديد السلوك الذي قد يكون هدفا للقانون الجنائي بشكل شرعي،[2] بيد أن التطبيق المنهجي لهذه المعايير على الأفعال السيبرانية قد يشكل تحديا. وبالرغم من ذلك، توجد دلائل في العديد من الأنظمة الوطنية، وفي بعض المبادرات الدولية والإقليمية تشير إلى عمل نظري يهدف إلى تعزيز تجريم السلوك السيبراني. ويشير التقرير التَفْسِيرِيّ لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، على سبيل المثال، إلى أن مفاهيم "المصالح القانونية" و"الأضرار" عرضة للخطر على نطاق واسع،[3] بالإضافة إلى ذلك، إذا كان هناك مبرر قوي لتجريم سلوك معين غير موجود، فإن ذلك يتمخض عنه خطر المغالاة في التجريم. وفي هذا الصدد، يوفر القانون الدولي لحقوق الإنسان أداة هامة لتقييم مدى مخالفة القوانين الجنائية لأحد المعايير الدولية الشكلية. ويتناول الفصل الرابع (التجريم) من هذه الدراسة مزيدا من أعداد الجريمة السيبرانية الشائعة ومقوماتها سواء في القانون الدولي أو في القانون الوطني.

---

[1] في حين أن–وفقا للقانون العام المعمول به في للدول–الكفاءات القضائية لتطوير وتوسيع نطاق القانون الجنائي يعتبر أمرا هاما بشكل تقليدي، إلا أن النُهُج الحديثة المعنية بالتجريم تتطلب الحالة القائمة على القانون حتى في أنظمة القانون العام الأساسية. أُنظر:

See *U.S. v. Hudson and Goodwin*, 11 U.S. 32 (1812); Dubber, M., 1999. Reforming American Penal Law. *Journal of American Criminal Law and Criminology,* 90(1)49-114; and Simester, A.P., Spencer, J.R., Sullivan, G.R., Virgo, G.J., 2010. *Criminal Law.* 4th ed. Oxford/Portland: Hart Publishing, p.46.

[2] بما في ذلك المفاهيم المتعلقة بالضرر والجريمة وعدم المشروعية، وحسن سلوك، السلطة الأبوية، السلع القانونية، والردع. أُنظر:

Ashworth, A., 2006. *Principles of Criminal Law.* 6th ed. Oxford: Oxford University Press, p.27; Dubber, H., 2005. Positive Generalprävention und Rechtsgutstheorie. *Zeitschrift für die gesamte Strafrechtswissenschaft,* pp. 485-518, pp.504 et seq.; Hassemer, W., 1980. *Theorie und Soziologie des Verbrechens.* Frankfurt a.M.; Feinberg, J. 1984. *Harm to Others.* Oxford: Oxford University Press

[3] مجلس أوروبا 2001، التقرير التفسيري للاتفاقية المعنية بالجريمة السيبرانية.

إلى جانب تجريم السلوك المحدد، يجب أن تضع أي دراسة معنية بالجريمة السيبرانية في اعتبارها القسم العام للقانون الجنائي، والذي يتناول عددا من الأمور التي تسري على جميع الجرائم، مثل المساهمة الجنائية، والشروع، والإهمال، والحالة الذهنية للمجرم (النية)، وحالة الدفاع الشرعي، والمسؤولية الجنائية للشخصيات الاعتبارية. وبصفة عامة، تخضع الجريمة السيبرانية إلى القسم العام لقانون العقوبات بنفس الطريقة التي تسري على أي جريمة أخرى. وفي هذا الصدد، أشارت العديد من الدول المجيبة على الاستبيان الملحق بالدراسة أن–على سبيل المثال–الجرائم الجنائية تقتصر على الأفعال المتعمدة، بشكل عام،[1] وبالرغم من ذلك؛ توجد إمكانية لتعديل هذه الأوضاع العامة لتتكيف مع أفعال معينة، مثل ضرورة توافر "نية محددة". ويتناول الفصل الرابع (التجريم) هذه المسألة بمزيد من التعمق.

الصلاحيات الإجرائية – كقاعدة عامة، لا يُتَصَوّر إجراء تحقيق فعال في إحدى الجرائم بدون صلاحيات استدلالية كافية، وعلة ذلك ترجع إلى طبيعتها المتداخلة، مما يستوجب ذلك أن ينظم القانون هذه الصلاحيات مع توفير تدابير وقائية كافة. بينما يمكن تنفيذ بعض إجراءات التحقيق بواسطة الصلاحيات التقليدية، إلا أنه يصعب تكييف العديد من القواعد الإجرائية التي تستند إلى نهج يقوم في توجّهه على الحيّز المكاني للأشياء لجعلها تستند إلى نهج يشمل تخزين البيانات الإلكترونية وتدفّق البيانات في الوقت الحقيقي. وبالتالي، تعتبر الصلاحيات التخصصية من الأمور الضرورية، ومثال على ذلك؛ عملية تَجْمِيع المحتوى الحاسوبي المنقول والمخزن إلكترونيا، ولتحديد وحصر أجهزة الحاسوب والمراسلات، ولتجميد سريع لبيانات الحاسوب المتَغَيّرة، ولإجراء التحقيقات السرية عبر الإنترنت.[2] ولا تكمن أهمية وجود هذه الصلاحيات للتحقيق فقط في "الجريمة السيبرانية" في حد ذاته، بل أيضا للتحقيق في أي جريمة تتولد عنها أدلة إلكترونية. هذا، ويتناول الفصل الخامس (التحقيقات وإنفاذ القانون) عددا من الصلاحيات التحقيقية المتخصصة الواردة في القوانين الدولية والوطنية.

جمع وإستعمال الأدلة – عادة ما يتضمن قانون الإجراءات الجنائية التقليدي أحكاما تتعلق بجمع الأدلة وقَبُولها، إلا أنه عندما تتخذ الأدلة الشكل الإلكتروني، فإنه من اليسير تغير بيانات الحاسوب. ولِهَذا؛ يجب عند جمع الأدلة الإلكترونية والتعامل معها ضمان الحيادية والصِحّة واستمراريتها خلال الفترة الزمنية بين توقيع الحجز عليها والأخذ بها في المحاكمة، وغالبا ما تعرف هذه العملية باسم "سلسلة المسؤوليات". وتشير الدول المجيبة على الاستبيان الملحق بهذه الدراسة إلى أن بعض الدول اتجهت إلى تقنين قواعد اسْتِدْلاليّة خاصة للأدلة الإلكترونية، في حين فضلت دول أخرى أن تتعامل مع الأدلة الإلكترونية بنفس الطريقة التي تتعامل بها مع أشكال الأدلة الأخرى. وفي الدول التي يأخذ فيها القانون العام بنظام المحلفين؛ فإن القوانين تتعامل بشكل مكثف مع الأدلة وقواعد قبولها، ومن ناحية أخرى، فإن الدول التي تطبق القانون الأوروبي تعتمد غالبا على مبدأ حرية القضاء في

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 40.

[2] Sieber, U., 2012. Straftaten und Strafverfolgung im Internet. *In*: *Gutachten des Deutschen Juristentags*. Munich: C.H. Beck, pp.C14-15.

تقييم أدلة الإثبات.[1] ويتناول الفصل السادس (العدالة الجنائية والأدلة الإلكترونية) مسألة الأدلة الإلكترونية بمزيد من التفصيل.

التنظيم والمخاطر – من المستقر قانونا، أن القانون الجنائي يركز على جلب المجرمين المسؤولين عن اقتراف أفعال سابقة ومثولهم أمام العدالة. ومن ناحية أخرى، تهدف القوانين التنظيمية والحد من المخاطر أو التعجيل إلى تقليل مخاطر الأفعال المستقبلية التي قد تحدث، أو جعلها أيسر لسلطات إنفاذ القانون لإجراء تحقيقات إنفاذ القانون وإجراءات العدالة الجنائية والتي يجب القيام بها.[2] أما فيما يتعلق بالجريمة السيبرانية، فإن عددا من الأساليب، منها تنقية الإنترنت، وحماية البيانات، واستعادة البيانات، وإجراء تحقيقات ابتدائية بشأن البنية التحتية للأعمال الإجرامية، تندرج ضمن هذه الفئة. وتجيز الطبيعة التَوَقّعِيّة للقوانين أن يكون العديد من هذه الإجراءات مكفولة بضمانات محددة، لكي تضمن أن هذه الإجراءات لن تمثل انتهاكات غير مناسبة لحقوق الأفراد، أو تنطوي على استخدام صلاحيات قَسْرِيّة بشكل غير ضروري.[3] ويتناول الفصل الثامن (المنع) عددا من هذه الأطر التنظيمية، من بين النواحي الأخرى للوقاية.

الولاية القضائية والتعاون الدولي – أفاد أكثر من نصف الدول المجيبة على الاستبيان الملحق بهذه الدراسة أن ما بين 50 و100 في المائة من أفعال الجريمة السيبرانية التي واجهتها الشرطة كانت تنطوي على عنصر "عابر للوطن".[4] وفي هذا الصدد، يجب على الدول أن: أولا: تؤكد قدرتها على تطبيق قوانينها الجنائية الوطنية على أي فعل يقع فقط بشكل جزئي، أو إن لم يكن كليا، داخل إقليمها الوطني، ثانيا: تبرز حاجتها إلى ما يمكنها من الاضطلاع بإجراءات التحقيق الذي قد يُجرى داخل إقليم دول أخرى. وفي حالة إذا اقتضت مجريات التحقيقات تجاوزات تمس سيادة الدول، فإنه يتعين في هذه الحالة الحصول على موافقة رسمية أو غير رسمية، بجانب إعمال التعاون الدولي في هذا الشأن. وتتجسد العديد من هذه الجوانب على مستوى القانون الدولي في شكل معاهدات ثنائية ومتعددة الأطراف، ومن ناحية ثانية يمكن أن تحدد القوانين الوطنية ماهية الإجراءات التي يجب تطبيقها أو تقنين قواعد للتعاون فيها. ويتناول الفصل السابع (التعاون الدولي) في هذا المجال بمزيد من التفصيل.

[1] Damaska, M.R., 1973. Evidentiary Barriers to Conviction and Two Models of Criminal Procedure: A Comparative Study. *University of Pennsylvania Law Review* 121(3):506-589 (1972-73).

[2] Sieber, U., 2012. Straftaten und Strafverfolgung im Internet. *In*: *Gutachten des Deutschen Juristentags*. Munich: C.H. Beck, note 1, pp.C 69-74.

[3] See European Commission. 2012. *Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, COM(2012) 9 final. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf

[4] الاستبيان الخاص بهذه الدراسة، السؤال رقم 83.

2-3 الاختلاف والمواءمة بين القوانين

الاستنتاجات الرئيسية:

- تعتبر المواءمة بين القوانين من الأمور الجوهرية، في جملة أمور، للقضاء على الملاذات الإجرامية وجمع الأدلة على الصعيد العالمي
- يستمد التباين في القوانين الوطنية المعنية بمكافحة الجريمة السيبرانية من مجموعة من العوامل، منها الاختلافات القانونية والدستورية الأساسية
- يجسد مجال العقوبات المقررة للجريمة السيبرانية مثالا جيدا على التباين في الأساليب الوطنية للتعامل مع أفعال الجريمة السيبرانية. ويُظهر تناول إحدى الجرائم – نفاذ غير مشروع – اختلافات كبيرة في تحديد درجة جسامتها
- ذكر ثلث البلدان المجيبة على الاستبيان الملحق بهذه الدراسة أن تشريعاتها تتسم بالمواءمة العالية، أو أشد من ذلك، مع البلدان الأخرى على اعتبار أن ذلك من الأمور الهامة لأغراض التعاون الدولي
- توجد درجة عالية من المواءمة حسبما أفادت عدد من الدول في أوروبا والأمريكتين، بالرغم من الاختلاف على المستوى الإقليمي
- قد يرجع ذلك إلى أن بعض المناطق تستخدم صكوكا متعددة الأطراف تمت صياغتها لتؤدي دورا ما في عملية المواءمة بين القوانين

إبراز الاختلافات بين القوانين

في ظل عالم تسوده العولمة، فإن أغلبية القوانين تتضمّن نظما قانونية وطنية وإقليمية ودولية، وعادة ما يحدث تفاعلات بين هذه النظم على مستويات متعددة، تؤدي إلى تعارض الأحكام لبعضها البعض في بعض الأحيان، أو اصطدامات بين القوانين، أو الإخفاق في التوافق بينهما بشكل كاف، أو تُحدث فجوات قضائية.[1]

لا تعتبر الجريمة السيبرانية بأي حال بمثابة أول نموذج إجرامي "جديد" يثير مسألة تنازع القوانين والاختصاص القضائي. ومثال على ذلك، فإن كثيرا ما يبدأ تدفق الاتجار في المخدرات والأسلحة بصورة غير مشروعة، علاوة على الاتجار بالبشر، وينتهي في مناطق مختلفة من نصف الكرة الأرضية، كما أنها تمر من بين العديد من الدول. وبالرغم من ذلك؛ يمكن أن تخضع أفعال الجريمة السيبرانية إلى نظم قانونية ضمن إطار زمني يقدر بجزء من ألف ثانية. ومثال على ذلك؛ يمكن أن يُخزن المحتوى الحاسوبي بشكل قانوني في أحد خوادم

[1] Sieber, U., 2010. Legal Order in a Global World. *In*: Von Bogdandy, A., Wolfrum, R. (eds.) *Max Planck Yearbook of United Nations Law*, 14:1-49.

الحاسوب في دولة ما، ولكن يتم تحميله عبر شبكة الإنترنت في بلدان متعددة، قد تعتبر أحد هذه البلدان أن المحتوى غير قانوني.[1]

وقد تولد عن حالة اختلاف الرؤى على الصعيد العالمي بشأن قبول أشكال محتوى الإنترنت عدد من البدائل النظرية. مما تمكنت الدول من اختيار ما تقيد به نطاق ولايتها القضائية في المسائل الجنائية لتسري على أنشطة الجناة التي يباشرونها على إقليمهم الوطني. ويمكن أن يركزوا على الملاحقة القضائية للأشخاص الذين قاموا بالنفاذ غير المشروع للمحتوى الحاسوبي داخل إقليمهم، وبغض النظر عن مصدره، أو يمكنهم الشروع في اتخاذ الإجراءات القانونية خارج الحدود الإقليمية ضد منتجي المحتوى، حيث توضح هذه المشْاهَد مدى تنامي الاختلافات القانونية والنهج المتبعة في مجال الجريمة السيبرانية. ويتناول الفصل الرابع (التجريم) هذه النقطة بتعمق أكثر، بالإضافة إلى تناولها من منظور القانون الدولي لحقوق الإنسان.

إختلافات التجريم – مثال لحالة

قام مواطن من إحدى الدول في أوقيانوسيا بتحميل مواد قانونية تتضمن أشكالا من خطاب الكراهية على أحد الخوادم في موطنه، وأتبع ذلك، أن هذه المادة قد تم تنزيلها في إحدى الدول الأوروبية. وعندما سافر هذا الشخص إلى تلك الدولة الأوروبية، أُلقي القبض عليه وحكم عليه بالسجن لارتكابه هذه الأفعال، التي لم تُجرّم في موطنه الأصلي. وقد تم استئناف القضية، حيث أيدت المحكمة الاتحادية العليا حكم الإدانة، وسببت ذلك؛ بأنه بالرغم من أن المتهم لم يقترف هذا الفعل في الدولة الأوروبية ولم يرسل بياناته إلى هذه الدولة بشكل متعمد، إلا أنه، مع ذلك، تسبب في تهديد السلم العام داخل الإقليم، على النحو المنصوص عليه في القانون ذي الصلة. ومع ذلك، أكدت المحكمة أن التفسير قد لا يمكن تعميمه للقوانين الأخرى بشأن محتوى غير قانوني.

المصدر:

Judgement of the German Bundesgerichtshof of 1 December 2000 (1 StR 184/00, please see BGH MMR 2001, pp.228 et seqq.)

يمكن أن ترجع بعض الاختلافات بين القوانين الوطنية إلى الفروق الجوهرية بين الأسر القانونية، حيث تنظم عادة وفقا للقانون القاري الأوروبي،[2] والقانون المدني،[3] والقانون الإسلامي،[4] والقانون المختلط (مثل القانون

[1] Sieber, U., 2008. Mastering Complexity in the Global Cyberspace. *In*: Delmas-Marty, M., Pieth, M., and Sieber, U. (eds.) *Les chemins de l'harmonization pénale*. Paris, pp.127-202 (192-197).

[2] غالبا ما يتسم القانون الجنائي القاري الأوروبي بوجود قواعد معيارية مجردة، وهياكل منهجية وتأثير قوى على الفكر الأكاديمي. ويعتبر القانون الجنائي عادة مُقَنّنا على نطاق واسع مع قوانين العقوبات، والتي تنص أيضا على المبادئ العامة للمسؤولية الجنائية التي تسري على كافة أشكال السلوك الإجرامي. أنظر:
Zweigert, K., Kötz, H. 1998. *Comparative Law*. 3rd ed. Oxford/New York: Clarendon Press, p.69. See also Weigend, T. 2011. *In*: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*, Stanford: Stanford University Press, pp.256 et seq.; Elliott, C., *ibid.*, p.213.; Gómez-Jara Díez, C., Chiesa, L.E., *ibid.*, p.493; Thaman, S.C., *ibid.*, p.416

[3] على النقيض من ذلك، ففي صلاحيات القانون المدني، تعتمد أحكام القوانين الموضوعية عادة على الصياغة الوصفية للمصطلحات، والتي تكفل كل من الوصول إلى القانون وتعكس قوة مركز القضاة غير المعيين الكامن في السلطة القانونية للقانون المدني. ومن ناحية أخرى لازالت التشريعات القضائية ومنذ زمن طويل المصدر الرئيسي للقانون الجنائي الموضوعي والذي يبقى حتى الآن عنصرا هاما. بيد أن التقنين مع ذلك يعتبر قاعدة واسعة الانتشار، وإن يكن من خلال قوانين تشريعية منفصلة بدل من قانون عقوبات منفرد. أنظر:
Legeais, R., 2004. *Grands systèmes de droit contemporains*. Paris: Litec, pp.357, 366; Ashworth, A. (United Kingdom). 2011, p.533, and also Robinson, P. (United States) 2011, p.564. Both *in*: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*, Stanford: Stanford University Press; Simester, A.P., Spencer, J.R., Sullivan, G.R., Virgo, G.J. 2010. *Criminal Law*. 4th ed. Oxford/Portland: Hart Publishing, p.46; Ashworth, A. 2009. *Principles of Criminal Law*. 6th ed. Oxford/New York: Oxford University Press, p.8.

[4] يعتبر القانون الإسلامي الموسوم بالشريعة الإسلامية بمثابة القانون المقدس للإسلام، بالإضافة إلى الفقه، والفقهاء المسلمين. وتصنف الجرائم طبقا لمصدرها القانوني والعقوبات المحددة لها، حيث يعاقب على عدد من الجرائم الأساسية من خلال استخدام العقوبات الثابتة (الحدود). بينما يُعاقب على الجرائم الأخرى من خلال

الصيني).[1] وتظهر ردود الدول على الاستبيان الملحق بهذه الدراسة أن هناك مجموعة كبيرة من النظم القانونية الممثلة.[2]

تعتبر الأسر القانونية بمثابة وسيلة هامة لتمييز التراث القانوني، بما في ذلك عندما تتشارك الأنظمة في سمات خاصة بسبب الجذور الثقافية المشتركة،[3] على سبيل المثال. ومع ذلك، لا تعتبر القوانين الوطنية ثابتة، كما أن التشابهات بين الأنظمة القانونية قد توجد عند نقطة محددة في وقت ما، ولكن تَتَوَارَى بعد ذلك.[4] وهكذا، يمكن أن تختفي الاختلافات التاريخية أو تفقد شأنها عمليا.

الشكل 3–2: تصنيف النظام القانوني الوطني للدول المجيبة على الاستبيان

القانون المدني 46%
نظام مختلط 28%
القانون العام 24%
القانون الإسلامي 2%

إستبيان دراسة الجريمة السيبرانية. السؤال 15. (رقم 54)

أما عندما يتعلق الأمر بالجريمة السيبرانية، تبقى بالتأكيد بعض الاختلافات القانونية التاريخية في قانون الإجراءات الجنائية الوطني مستمرة.[5] وبالرغم من ذلك، تتوقف الاختلافات في المضمون العام للقانون الجنائي بصورة أقل مما هي عليه في الأحكام القانونية الخاصة بالأحوال الشخصية، سواء كان ذلك في القانون المدني أو القانون العام، كما تساهم الأمور الاجتماعية والثقافية والدستورية السائدة بصورة أكبر في هذه الاختلافات. وفي هذا الصدد، يؤكد هذا التباين، على سبيل المثال، على قيم الخصوصية وحرية التعبير، أو على الفرد أو المجتمع، والذي يمكن أن يصاحبه تأثير بليغ على نتائج السياسة والتجريم. أما في سياق الجريمة السيبرانية؛ فإن هذا الأمر قد يقود إلى نتائج قانونية مختلفة في مجالات مثل: ضَبْط المواد المخلة بالآداب،[6] والتوازن بين حرية التعبير والتعبير غير

الاستدلال القانوني على أساس الإجماع والقياس. وبصفة عامة، تسمح القوانين الإسلامية بمرونة واسعة فيما يتعلق بالتجريم، بما في ذلك من خلال تطور المدارس الفقهية المختلفة للقانون. أنظر:
Tellenbach, S., 2011. *In*: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*. Stanford: Stanford University Press, p.321.

[1] لقد تأثر القانون الجنائي الصيني بمجموعة واسعة من النظم القانونية، حيث تحتفظ السلطة القضائية بصلاحية هامة لإعطاء تفسيرات قضائية الزامية للقانون. أنظر:
Luo, W., 2011. *In:* Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law.* Stanford: Stanford University Press, p.138; and Bu, Y., 2009. *Einführung in das Becht Chinas.* Munich: C.H. Beck, p. 20.

[2] الاستبيان الخاص بالدراسة، السؤال رقم 15.

[3] See Ferrante, M., 2011. *In:* Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*. Stanford: Stanford University Press, p.13.

[4] Zweigert, K., Kötz, H. 1998. *Comparative Law.* 3rd ed. Oxford/New York: Clarendon Press, p.66.

[5] On the evolving and heterogeneous nature of procedural law, see Legeais, R., 2004. *Grands systèmes de droit contemporains*. Paris: Litec, p.389.

[6] See, for instance, Segura-Serrano, A., 2006. Internet Regulation and the Role of International Law. *In*: Von Bogdandy, A., Wolfrum, R. (eds.) *Max Planck Yearbook of United Nations Law*, 10(2006):191-272; Edick, D.A. 1998. Regulation of Pornography on the Internet in the United States and the United Kingdom: A Comparative Analysis. *Boston College International & Comparative. Law Review* 21(2):437-460.

المقبول،[1] ومستويات الوصول إلى محتوى الإنترنت،[2] وقواعد والتزامات مقدمي خدمة الإنترنت،[3] والضمانات والقيود المفروضة على تدخل تحقيقات إنفاذ القانون.[4]

بالإضافة إلى التأثيرات الاجتماعية والثقافية والدستورية، فإنه لا يجب التقليل من الواقع الذي تتركه عمليات الصياغة القانونية للمصادفات التاريخية البسيطة، وتأثير الرؤى الفردية للخبراء، والتقييمات المتباينة لأفضل الممارسات. وأخيرا، فإن الاختلافات القانونية التقنية الناتجة عن هذه التأثيرات، فضلا عن التراث الإجرائي القانوني، قد تكون إلى حد كبير أكثر وضوحا للتصدي لما ينبثق عن المستويين الاجتماعي-الثقافي والدستوري.

مواءمة القوانين

تؤدي هذه الاختلافات إلى إثارة تساؤل؛ عما إذا كان من المتعين الحد من الاختلافات القانونية الوطنية في قوانين مكافحة الجريمة السيبرانية والعمل على تقليلها، وإذا كان الأمر كذلك، إلى أي مدى يمكن فعل ذلك. وبعبارة أخرى؛ ما هي أهمية إعمال مواءمة بين القوانين المعنية بالجريمة السيبرانية؟ حيث توجد عدة طرائق حيال ذلك، من خلال الالتزام بكل من المبادرات الدولية أو الإقليمية أو عدم الالتزام بأي منهما.وقد يتجسد أساس المواءمة بين القوانين في نهج وطني منفرد (مع تنقيح كافة قوانينهم لتتماشى مع المواءمة)، أو في كثير من الأحيان، العناصر القانونية السائدة المحددة في عدد من قوانين الدول، أو قد يكون معبرا عنه في أحد الصكوك متعددة الأطراف، مثل اتفاقية أو معيار دولي غير ملزم. وفي الواقع، وعلى النحو الوارد أدناه، فإن أحد أهداف القانون الدولي يتمثل في تحقيق المواءمة بين القوانين الوطنية.

وفي أثناء جمع المعلومات لهذه الدراسة، قد وجه تساؤل للدول حول الدرجة المتصورة للمواءمة بين التشريعات المعنية بالجريمة السيبرانية، وكذلك عن ماهية النجاحات التي حققتها هذه المواءمة والقيود المفروضة عليها، إلى جانب ذلك، ما هي الأساليب المستخدمة للحفاظ على التقاليد القانونية أثناء إجراء عملية المواءمة بين القوانين.[5] وفي هذا الشأن، أبرز عدد من دول آسيا والأمريكتين على وجه الخصوص؛ أنه بينما اعتبرت عملية المواءمة أمرا هاما، إلى أنها قد تخضع إلى بعض القيود الضرورية، منها "*التنازع مع المتطلبات الدستورية*"، في حين أن متطلبات المواءمة تقضي بعدم وجوب "*تعارض بينها وبين والأسس العامة للقانون والشريعة*"، ومن ثم تبرز الحاجة إلى "التطبيق السياقي" للمعايير المنظمة، بالإضافة إلى قضايا وجود تشريعات على المستويين الاتحادي ومستوى الولايات داخل إحدى الدول.[6] وفي هذا السياق؛ أبلغت أيضا الدول عن نجاحات في إجراء مواءمة بين

---

[1] See *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/67/357, 7 September 2012

[2] المرجع السابق

[3] See *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/17/27, 16 May 2011.

[4] فيما يتعلق على سبيل المثال بالتحقيقات في استعمال الحاسوب في أعمال دعم الجرائم الإرهابية، أنظر مكتب الأمم المتحدة المعني بالجريمة والمخدرات 2012، استعمال الإنترنت في الأغراض الإرهابية، الفقرات 35،106، 110

[5] الاستبيان الخاص بالدراسة، السؤال رقم 16، و17

[6] المرجع السابق، السؤال رقم 16.

التشريعات المعنية بالجريمة السيبرانية، كما أوضحت، على سبيل المثال، أن عملية المواءمة تعتبر جزءا من "*نهج متكامل لإدراج القواعد الموضوعية والإجرائية للقانون*"، وأنه يمكن أن الحفاظ على التقاليد القانونية الوطنية من خلال "*الأخذ بعين الاعتبار خصوصية المجتمع المتعلقة بالعادات والتقاليد والأعراف* [و] *والتشريعات الوطنية الموجودة سلفا*".[1]

وأفادت الدول المجيبة على الاستبيان الخاص بهذه الدراسة بأن درجة المواءمة بين قوانين مكافحة الجريمة السيبرانية تختلف اختلافا كبيرا وفقا للإقليم، بجانب ما إذا كانت المواءمة تتعلق بـ (1) دول أخرى، أو (2) داخل الإقليم، أو (3) بناء على الأحكام الواردة في الصكوك متعددة الأطراف. وبإيجاز؛ يبين الشكل 3-3 أدناه، أن ما يقرب من ثلث الدول ذكرت أن تشريعاتها اتسمت بالمواءمة "العالية الى درجة كبيرة" أو "إلى حد كبير" مع تشريعات الدول الأخرى. أما النسبة الباقية من الدول، فترى أن تشريعاتها تعتبر "جزئيا" أو "نوعا ما" متوائمة مع تشريعات الدول الأخرى. هذا، وتشكل مستويات المواءمة المتصورة في أوروبا والأمريكتين نسبة أعلى من تلك الموجودة في أفريقيا وآسيا وأوقيانوسيا. وقد عنيت إحدى الدول الآسيوية بالتعليق مباشرة بأن "*لا تعتبر التشريعات الحالية متوافقة مع الدول التي تشكل أهمية للأغراض التعاون الدولي*"،[2] بينما أشارت الدول الأخرى إلى الموقف العالمي من هذه المسألة. ومن ناحية أخرى أفادت إحدى الدول الأوروبية، على سبيل المثال، بأنه "*يوجد على المستوى الإقليمي درجة عالية من المواءمة، وهذا لم يتسن لنا التأكد منه على الصعيد العالمي. وبالرغم من ذلك، لم يُرفض لنا [بَعْد] طلب للتعاون الدولي في مجال القضاء على أساس عدم توافر متطلبات التجريم المزدوج، مما يستجلي أن اختلاف القواعد الإجرائية [الموجودة] تتعلق بالتعاون القضائي الدولي*".[3]

علقت العديد من الدول على مدى فائدة الصكوك الدولية في عملية المواءمة بين القوانين، فعلى سبيل المثال، أفادت إحدى الدول أنه من المفيد أن تكون لدينا معايير خارجية مثل تلك الموجودة في الصكوك الدولية والإقليمية، "*التي يمكننا مقارنة الأحكام الواردة في قوانيننا معها*".[4] كما ذكرت إحدى الدول الأخرى بأن المنتديات الدولية تسعى لتوافق الآراء بشأن الاستراتيجيات الدولية والتدابير القانونية ضد الجريمة السيبرانية، إذ توفر "*فُرصا لتبادل الأفكار التي يمكن أن تتخذها أي دولة طرف كفائدة تشريعية أو كخيارات عملية لمنع الجريمة ومكافحتها*". ورأت نفس الدولة أن عمليات المواءمة ما هي إلا عملية ذات اتجاهين، كما "في بعض الحالات، حيث أن المبادرات التشريعية المحلية أو الأفكار تعتبر بمثابة مصدر العناصر في المعايير الدولية، وفي حالات أخرى، أثرت الأفكار التي عبرت عنها دول أعضاء أخرى على عملية النَظَر [محليا] في الجريمة السيبرانية، واستطاعت أن تجد سبيلها إلى إلى القوانين [الوطنية] نتيجة لذلك".[5]

---

[1] المرجع السابق

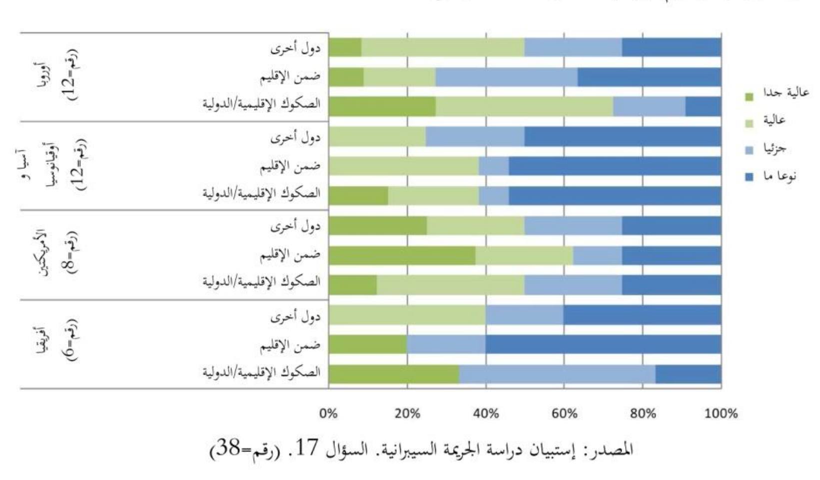
[2] الاستبيان الخاص بالدراسة، السؤال رقم 17

[3] المرجع السابق.

[4] الاستبيان الخاص بالدراسة، السؤال رقم 16

[5] الاستبيان الخاص بالدراسة، السؤال رقم 17

الشكل 3-3: درجة المواءمة لتشريعات الجريمة السيبرانية مع: (1) الدول الأخرى المهمة للتعاون، و(2) الإقليم، و(3) الصكوك متعددة الأطراف



المصدر: إستبيان دراسة الجريمة السيبرانية. السؤال 17. (رقم=38)

واستكمالا لهذا السياق، فقد لاحظت دول أخرى تأثير التشريعات الوطنية الموجودة. وذكرت إحدى دول شرق آسيا، على سبيل المثال، أنها "*قد قامت بدراسة التشريعات الأجنبية لوضع تشريعاتها الوطنية*".[1] وإجمالا، فإن الشكل 3-3 يعتبر بالأحرى غير قاطع لتأثير الصكوك الدولية على عمليات المواءمة. وتجدر الإشارة إلى أن المستويات العالية من المواءمة المتصورة بين التشريعات الوطنية والصكوك الدولية في دول أوروبا، على سبيل المثال، لا تكشف عن ترجمة مباشرة لمستويات المواءمة العالية مع الدول داخل الإقليم.

ويتناول هذا الفصل لاحقا تأثير الصكوك الدولية ذات الصلة بالجريمة السيبرانية على التشريعات الوطنية.

ومع ذلك، ينبغي أولا دراسة الأسباب والأسس المنطقية وراء المواءمة بين التشريعات المعنية بمكافحة الجريمة السيبرانية.

لماذا المواءمة؟

لتجنب الملاذات الآمنة – تكمن الميزة الرئيسية لمواءمة القانون الجنائي في مجال الجريمة السيبرانية، ولكل الجرائم التي ترتكب عبر الحدود الوطنية، في منع وجود ملاذات آمنة لمرتكبي الجريمة السيبرانية. وكما أفادت إحدى الدول المجيبة على الاستبيان الخاص بهذه الدراسة فأن "*الجريمة السيبرانية تعتبر ظاهرة عالمية، مما يجعل كل الدول هامة بالنسبة لنا بشكل من اشكال مختلفة... حيث نعتقد أن التعاون مع الدول النامية يمثل أهمية خاصة على أساس أن الجريمة السيبرانية لا تعرف حدودا*".[2] وفي الواقع، فإن الجريمة السيبرانية تشكل على الأرجح خطورة مباشرة بشكل كبير نظرا لأنها تمنح ملاجئ آمنة للجناة، مقارنة مع كل الجرائم عبر الحدود الوطنية.

وبالتالي، إذا جُرمت الأفعال الضارة المشتملة على الإنترنت، على سبيل المثال، في الدولة (أ)، ولكنها غير مجرمة في الدولة (ب)، فإن أحد الجناة في الدولة (ب) يكون طليقا في استهداف الضحايا في الدولة (أ) عبر الإنترنت. وفي هذه الحالات، لا تستطيع الدولة (أ) أن تقوم من تلقاء نفسها ببسط حماية فعالة ضد الآثار المترتبة

[1] الاستبيان الخاص بالدراسة، السؤال رقم 16

[2] الاستبيان الخاص بالدراسة، السؤال رقم 17

على هذه الأنشطة العابرة للحدود الوطنية، حتى وإن كان قانونها الجنائي يسمح بسريان الولاية القضائية على الأفعال التي يرتكبها الجاني في الدولة (ب)، إلا أن ذلك مرهون بموافقة أو مساعدة من الدولة (ب)، سواء تعلق الأمر بجمع أدلة أو تسليم مرتكب الجريمة التي تم تحديدها، كما أنه من غير المرجح أن تضطلع الدولة (ب) من أجل حماية أشخاص داخل نطاق ولايتها القضائية بالمساعدة إذا كان السلوك غير مجرم أيضا في إقليمها، حيث يعتبر مبدأ التجريم المزدوج الأساس في العديد من أشكال التعاون الدولي. وقد يوجد ذلك، على سبيل المثال، في معاهدات تسليم المجرمين الثنائية ومتعددة الأطراف، فضلا عن القوانين الوطنية.[1]

يجسد التجريم المزدوج دورا في المساعدة القانونية المتبادلة، مثل طلبات استجواب الشهود، أو جمع الأدلة.[2] بينما لا تشترط كل الاتفاقيات بين الدول بشأن المساعدة القانونية المتبادلة التجريم المزدوج، إلا أن العديد من الصكوك تؤكد على أن التدابير القسرية أو التدخلية مثل التفتيش والمصادرة أو تجميد الممتلكات تخضع لشرط التجريم المزدوج،[3] ويتناول الفصل السابع (التعاون الدولي) هذا المبدأ بمزيد من التفصيل. ومع ذلك، ولأغراض المواءمة بين القوانين الجنائية المعنية بالجريمة السيبرانية، فإن أحد النقاط الهامة تتمثل في عدم اشتراط التجريم المزدوج أن يكون النشاط الأساسي معاقبا عليه بنفس النمط للحكم القانوني. وبالتالي، إذا كانت الدولة (ج) تستخدم سلوكا معينا تقوم عليه جريمة سيبرانية محددة، في حين أن الدولة (د) تستخدم الجريمة العامة، فإن كلا الدولتين تستطيع أن تبادر في التعاون الدولي، شريطة أن تكون الأركان الرئيسية للجريمة قابلة للمقارنة بموجب قانون كل من الدولتين.[4] على النحو الذي تناوله الفصل السابع، إذا حققت الدول درجة معينة من المواءمة بين قوانينها الوطنية (مثلما حدث في الاتحاد الأوروبي)، فإن مبدأ التجريم المزدوج قد يحل محل الخلل الافتراضي في تكافئ القوانين.[5]

لتمكين جمع الأدلة على الصعيد العالمي – تعتبر المواءمة بين القوانين الإجرائية متطلبا ثانيا ضروريا للتعاون الدولي الفعّال. ففي المثال المذكور أعلاه؛ إذا لم يكن – على سبيل المثال – لدى الدولة (ب) الصلاحية

---

[1] أُنظر على سبيل المثال، الفقرة 1 من المادة (2) من معاهدة الأمم المتحدة النموذجية لتسليم المجرمين، والفقرة (1) من المادة 2 من الاتفاقية الأوروبية لتسليم المجرمين، والمادة (2) من خطة لندن لتسليم المطلوبين داخل الكومنولث.

أُنظر أيضا:

Plachta, M., 1989. The role of double criminality in international cooperation in penal matters. *In*: Agell, A., Bomann, R., and Jareborg, N. (eds.) *Double criminality, Studies in international criminal law*. Uppsala: Iustus Förlag, p.111, referring to, *inter alia*, Shearer, I., 1971. *Extradition in international law*. Manchester, p. 137, and Bassiouni, M.C., 1974. *International extradition and world public order*. Dordrecht: Kluwer Academic Publishers, p.325

[2] أُنظر: Capus, N., 2010. *Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen*. Bern: Nomos, p.406.

[3] أُنظر على سبيل المثال: المادة 5(1) من اتفاقية مجلس أوروبا بشأن المساعدة القانونية المتبادلة، والمادة 18(1) (و) من اتفاقية مجلس أوروبا بشأن غسل الأموال والتفتيش والاستيلاء عليها ومصادرة العائدات المتأتية من الجريمة. ولتبادل المعلومات أو غير ذلك من أشكال التعاون الذي لا يشكل تعديا على حقوق الشخص المعني، ولم يشترط التجريم المزدوج. أُنظر:

See Vermeulen, G., De Bondt, W., Ryckman, C., 2012. *Rethinking International Cooperation in Criminal Matters in the EU*. Antwerp: Maklu, p.133; and Klip, A., 2012. *European Criminal Law*. Antwerp: Intersentia, p.345.

[4] Plachta, M., 1989. The role of double criminality in international cooperation in penal matters. *In*: Agell, A., Bomann, R., Jareborg, N. (eds.). *Double criminality, Studies in international criminal law*. Uppsala: Iustus Förlag, pp.108-109. See also: *Explanatory report to the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime,* that specifies in the clarification of Art. 18(1)(f) that dual criminality is required in abstract to for the investigative measures meant by Section 2, which includes (but is not limited to) the investigative measures that require coercive action.

[5] See De Bondt, W., 2012. *Need for and feasibility of an EU offence policy*. Antwerp: Maklu, pp. 46-47.

الإجرائية اللازمة للتحفظ العاجل على البيانات الحاسوبية، ومن ثم، فالدولة (أ) لن تتمكن من طلب هذه المصلحة من خلال المساعدة القانونية المتبادلة. وبعبارة أخرى؛ فإن الدولة الموجه إليها الطلب تتمكن فقط من تقديم المساعدة داخل إقليمها إلى الحد الذي يمكنها من أداء ذلك لإجراء تحقيق وطني مكَافِئ.[1] مرة أخرى، فيما يتعلق بالتجريم المزدوج، فإن الشكل القانوني للصلاحية الإجرائية لا يشترط أن يكون مُتَوَازِيا مباشرة، طالما توجد إمكانية لإجراء التحقيق عمليا. وغني عن البيان، أن تَوْفِير التحفظ العاجل على البيانات، على سبيل المثال، قد يتحقق بصورة شرعية إما عن طريق نظام مُخَصّص أو سلطة عامة منوط بها البحث والمصادرة.

للتعبير عن "خطورة الجريمة" والتقليل من "الملاذات الجزائية" – وفقا لمنظور التعاون الدولي، فإن العقوبات المحددة للجرائم الجنائية لا تتطلب بشكل دقيق المواءمة بين نفس الأسس التي ينتهجها القانون الجنائي الموضوعي والصلاحيات القسرية لقانون الإجراءات الجنائية، إلى جانب ذلك، فإن مبدأ التجريم المزدوج لا يتعلق بالعقوبات ذات الصلة. بيد أن هناك رابطا، بالرغم من ذلك، بين التعاون ومستوى العقوبة المفروضة، حيث تعتبر العقوبات المقررة لإحدى الجرائم ذات دَلَالَة بمستوى جسامة الجريمة. أما على المستوى الدولي، على سبيل المثال، فقد تعرف اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية "الجريمة الخطيرة" بأنها سلوك يمثل جرما "*يعاقب عليه بالحرمان التام من الحرية لمدة لا تقل عن أربع سنوات أو بعقوبة أشد*".[2] وفي ضوء الفوائد الكبيرة المفترَضة التي تتطلب تعاونا دوليا من الدول، فإن العديد من الصكوك المعنية بتسليم المجرمين المطلوبين تحدد درجة خطورة الجريمة المرتكبة، وعادة ما يعبر عن ذلك بالإشارة إلى العقوبة المحتملة التي تستدعيها الجريمة.[3] ومن ناحية أخرى، تقدم أيضا درجة خطورة الجريمة آلية هامة لحماية مبدأ التناسب وحقوق المتهم،[4] وقد يطبق أيضا شرطا مماثلا في بعض الاتفاقيات بشأن بالمساعدة القانونية المتبادلة.[5]

ويوجد حد نمطي للعقوبة في صكوك التعاون الدولي تتراوح مدتها من ستة أشهر،[6] إلى سنة واحدة،[1] أو أربع سنوات.[2] وخلال جمع المعلومات الخاصة بهذه الدراسة، قد سُئلت الدول عن العقوبات التي تطبق على

[1] عادة لا يذكر ذلك صراحة في الصكوك التي تنظم المساعدة القانونية المتبادلة، حيث أن الإجراءات التي لا توجد في الدولة المطلوب منها تقديم المساعدة، وبالرغم من ذلك يتعين تنفيذ هذه الإجراءات. وبالنسبة للإجراءات القصرية، مع ذلك، ينص مشروع نظام التحقيق الأوروبي على أنه يجوز اللجوء إلى الإجراءات البديلة، وينبغي ذلك، عندما لا توجد الإجراءات المطلوبة بموجب قانون الدولة الموجه إليها الطلب. أنظر مجلس أوروبا 2011. مبادرة الأمر التوجيهي بشأن نظام التحقيق الأوروبي في المسائل الجنائية–تمت الموافقة على النص كاتجاه عام، أمر توجيهي رقم 18918/11، كانون الأول/ديسمبر 2011، الصفحات 19-20.

[2] قد استخدمت المادة الثانية من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية حد أربع سنوات لوضع تصنيف عام "للجريمة الخطيرة" التي تسري عليها الاتفاقية (والتي يجب أن تتخذ طبيعتها شكل الجرائم عبر الحدود الوطنية، بالإضافة إلى ضلوع جماعة إجرامية منظمة في ارتكابها)، ولا يسري هذا الحد على الجرائم الخاصة أيضا المقننة في الاتفاقية.

[3] Schwaighofer, K., Ebensperger S., 2001. *Internationale Rechtshilfe in strafrechtlichen Angelegenheiten.* Vienna: WUV Universitätsverlag, p. 8.

[4] Lagodny, O. 2012. *In:* Schomburg, W., Lagodny, O., Gless, S., Hackner, T. (eds.) *Internationale Rechtshilfe in Strafsachen.* Munich: C.H.Beck, p.90 § 3 IRG, at 23; Murschetz, V. 2007. *Auslieferung und Europäischer Haftbefehl.* Vienna/New York: Springer, p.124.

[5] المادة 5 (1) (ب) من الاتفاقية الأوروبية بشأن المساعدة القانونية في المسائل الجنائية، على سبيل المثال، تنص على أنه يجوز لأي طرف متعاقد أن يطلب تسليم مجرمين مطلوبين في ارتكاب إحدى الجرائم من أجل تنفيذ الإنابة القضائية للبحث ومصادرة الممتلكات.

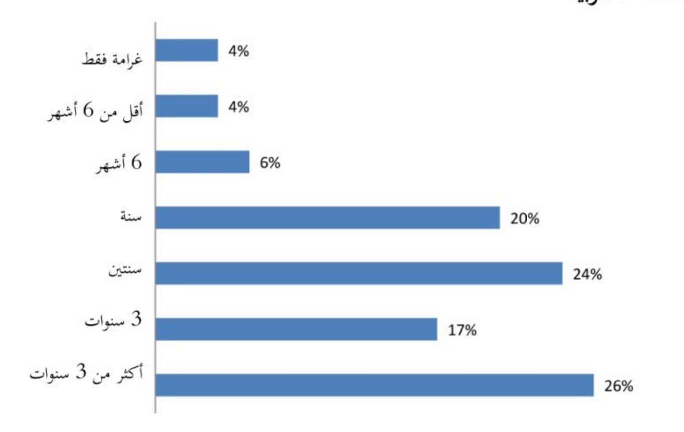
[6] المادة 2 (1) من اتفاقية الاتحاد الأوروبي بشأن تسليم المجرمين تنص على أن الجريمة التي يخضع مرتكبها للتسليم إذا كان معاقبا عليها بسلب حرية الجاني بمدة سنة واحدة على الأقل بموجب قانون الدولة الطالبة وستة أشهر بموجب قانون الدولة الموجه إليها الطلب. ويلاحظ مع ذلك، أن الاتفاقية قد استبدلت ذلك بمذكرة التوقيف الأوروبية. أنظر:

مجموعة من أفعال الجريمة السيبرانية، بما في ذلك تلك المرتكبة ضد السرية، والنزاهة، وتوافر بيانات حاسوبية أو نظم حاسوب، وكذلك الأفعال ذات الصلة بالحاسوب والتي تهدف إلى تحقيق مكاسب شخصية أو مالية، والأعمال الخاصة ذات الصلة بالحاسوب.[3]

تبين الأشكال 3-4، و3-5، توزيع العقوبات المقررة لأفعال "النفاذ غير المشروع" لنظام الحاسوب أو البيانات الحاسوبية، ولنفس الجريمة، ولكن في حالة "تجاوز الأمن" أو "نوايا غير شريفة"، فإن ذلك يتطلب حكما قانونيا وطنيا،[4] خاص بهما.

ومن الجلي لكلا الجريمتين، أن عددا من الدول تنص على عقوبات بحد أقصى سنة واحدة أو أقل، في ظل حقيقة مؤداها أن عقوبة سنة واحدة تعتبر في الغالب العقوبة الأكثر شيوعا لأغراض تسليم المجرمين المطلوبين (وقد أدرجت بعض الصكوك هذه العقوبة، مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، واتفاقية الدول العربية)، ويلاحظ أن التعاون الدولي في مجال هذه الجرائم (مفردة) في بعض الدول قد يشكل تحديا.[5] هذا، ويعتبر الحكم النمطي أقل بكثير من أربع سنوات "للجرائم الخطيرة" الوارد في اتفاقية الجريمة المنظمة.

الشكل 3-4: الحد الأقصى لعقوبة السجن لمجرد النفاذ غير المشروع لنظام أو بيانات حاسوبية



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة (رقم=54)

(Hackner, T., 2012. *In:*, Schomburg, W., Lagodny, O., Gless, S., Hackner, T. (eds.) *Internationale Rechtshilfe in Strafsachen*. Munich: C.H.Beck. p.1174, III A, at 3, and pp.1178-1179, III A 1, at 9).

[1] أحكام تسليم المجرمين الواردة في اتفاقية مجلس أوروبا بشأن الجرائم السيبرانية، على سبيل المثال، تسري على الجرائم الجنائية الواردة فيها وفقا للمواد 2 إلى 11 من الاتفاقية، شريطة أن يكون معاقبا عليها بموجب قوانين كلا الطرفين بالحرمان من الحرية لمدة أقصاها سنة واحدة على الأقل، أو بعقوبة أشد.

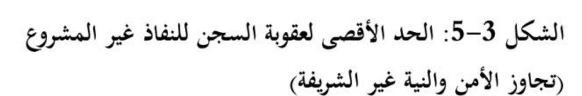
[2] اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المواد 2، و16

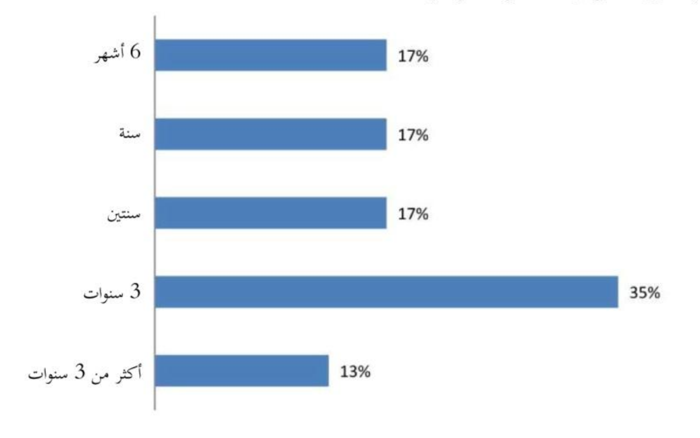
[3] الاستبيان الخاص بالدراسة، السؤال رقم 25-39. قد جمعت المعلومات بشأن العقوبات من قبل الأمانة العامة من مصادر إضافية مدرجة في استعراض المصدر الرئيسي للتشريعات.

[4] اقتصر التحليل على الدول التي تشير إلى الحد الأقصى للعقوبة في مادة قانونية محددة (بالتالي لم يتضمن التحليل الدول التي يمكن أن تحدد العقوبة من خلال تحليل الأحكام العامة للقانون الجنائي).

[5] على الرغم من ملاحظة أن الدول المجيبة على الاستبيان أفادت أيضا بأن الأفعال التي تشكل الجريمة السيبرانية تعتبر ذات نطاق واسع وتفي بمعايير الجسامة وتشكل جرائم يخضع مرتكبوها للتسليم. كما أفادت جميع دول أوروبا والأمريكتين، وما يقرب من 90 في المائة من دول أفريقيا وآسيا وأوقيانوسيا أن أعمال الجريمة الإلكترونية تعتبر جرائم قابلة لتسليم مرتكبيها (الاستبيان الخاص بالدراسة، السؤال رقم 194). وقد يرجع سبب التناقض المحتمل إلى أن حقيقة مؤداها أنه من النادر توجيه الاتهام للجناة- وطلب تسليمهم-بالنفاذ غير المشروع بمعزل عن التهم الأخرى.

ومع ذلك، فإنه ينبغي تفسير هذه النتائج مع التَحَفّظ فيما يتعلق بمشهد العقوبات المطبقة عمليّا، حيث لا يمكن، من الناحية العملية، تقييم مستويات العقوبة بمعزل عن أحكام القانون الجنائي المعنية بذلك. وبالأحرى، قد تتأثر مستويات العقوبة بالقواعد العامة للحكم القضائي أو بالظروف المشَدِّدة والمخففة، أو بالمبادئ التوجيهية للحكم القضائي والمتطلبات المحددة.


الشكل 3-5: الحد الأقصى لعقوبة السجن للنفاذ غير المشروع
(تجاوز الأمن والنية غير الشريفة)



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة (رقم=23)

وبالرغم من ذلك، فإن المشهد يلقي الضوء على التحديات العامة التي برزت عندما تعلق الأمر بتحديد نطاق التعاون الدولي والاتفاقيات المشتركة بشأن خطورة الجريمة السيبرانية. فمن ناحية، يمكن أن يغطي فعل "مجرد النفاذ غير المشروع" سلوكا ضئيلا بشكل نسبي، ومن ناحية أخرى، فإن النفاذ غير المشروع يعتبر مدخلا لنقطة انطلاق العديد من أفعال الجريمة السيبرانية التي تشكل خطورة، كذلك من الجائز أن يشمل النفاذ المتعمد غير المأذون به على الدخول إلى نظم الحاسوب، مثل تلك المستخدمة للبنية التحتية الوطنية بشكل أساسي. وفيما يتعلق بـ "الحد الأقصى" للحكم الجزائي المحتمل لأغراض تحديد حد التعاون، فإن وصف الفعل ذاته بشكل جيد لا يشكل أمرا ضروريا. بيد أن الأساليب البديلة تعاني من نطاق القيود المفروضة، مثل تحديد قائمة الجرائم الخاصة التي تكون محل أحكام التعاون الدولي (بدون حاجة لحدود جزائية). وأخيرا، وبشكل مجمل، فإن المواءمة الكُلّيّة للعقوبات بين الدول لجرائم سيبرانية محددة وأساسية – بما في ذلك مستويات العقوبة القائمة على خطورة تقليدية – يمكن أن تساهم على الأرجح في المساعدة على تيسير التعاون الدولي والقضاء على "الملاذات الجزائية" لمرتكبيها.

ملخّص

تعتبر الصورة الحالية للتشريعات المعنية بمكافحة الجريمة السيبرانية إحدى الصور الفَعّالة، كما تعبر عن الإصلاحات القانونية المستمرة المتزامنة مع تصاعد الإقرار بأن الجريمة السيبرانية تتطلب استجابة قانونية تغطي المجالات الجنائية والمدنية والإدارية المتعددة. وقد أشار ما يقرب من 60 في المائة من الدول المجيبة على الاستبيان الخاص بالدراسة إلى أن وجود تشريعات جديدة أو خطط لسن تشريعات تواجه الجريمة السيبرانية.[1] وبينما يمكن تطبيق القانون العام "التقليدي" على الأمور المتعلقة بالجريمة السيبرانية إلى حد ما، إلا أن الطبيعة المعنوية للمفاهيم،

[1] الاستبيان الخاص بالدراسة، السؤال رقم 14

مثل "البيانات الحاسوبية"، تتطلب أيضا مدخلا يستوعب الجرائم المحددة والتعريفات والمفاهيم، وذلك في حالة إذا كانت المصالح القانونية (مثل: سلامة أنظمة الحاسوب) محمية.

وبينما يوجد توافق في الآراء بشأن المجالات الواسعة للتدخل القانوني لمنع ومكافحة الجريمة السيبرانية، إلا أنه يُنظر إلى مستويات مواءمة التشريعات بين الدول كعنصر هام — ومتغير بصورة كبيرة – للتعاون داخل الأقاليم، ومع الصكوك متعددة الأطراف. وهذا يشتمل على مجال العقوبات المقررة للجريمة السيبرانية، حيث يظهر تناول إحدى الجرائم التأسيسية – النفاذ غير المشروع – اختلافا إلى حد يؤثر على سهولة التعاون الدولي بشأن هذه الجريمة. فمن المستقر أن عمليات المواءمة نفسها مطلوبة لعدة أسباب منها؛ القضاء على الملاجئ الآمنة للجناة وجمع المعلومات على الصعيد العالمي. وختاما، فإن طرائق المواءمة تتضمن استعمال الصكوك الدولية والإقليمية الملزمة وغير الملزمة، حيث ألمحت هذه الدراسة إلى العديد من هذه الصكوك الموجودة حتى الآن. ويتناول القسم التالي من هذا الفصل هذه النقاط بمزيد من التفصيل.

3-3 نظرة عامة على الصكوك الدولية والإقليمية

الاستنتاجات الرئيسية:

- لقد شهد العقد الماضي تطورات هامة في صدور صكوك دولية وإقليمية رامية إلى مكافحة الجريمة السيبرانية، ويتضمن ذلك الصكوك الملزمة وغير الملزمة
- يمكن تحديد خمس مجموعات من الصكوك الدولية أو الإقليمية، مركبة من صكوك وضعت في سياق، أو مستوحاة من اتفاقيات: (1) مجلس أوروبا أو الاتحاد الأوروبي، (2) كومنولث الدول المستقلة أو منظمة شنغهاي للتعاون، (3) المنظمات الحكومية الدولية الأفريقية، (4) جامعة الدول العربية، (5) الأمم المتحدة
- يوجد قدر كبير من التقاسم بين كل جميع الصكوك، بما في ذلك، وبصفة خاصة وضع المفاهيم والنهج المستخدمة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية
- يظهر تحليل أحكام 19 صكا من الصكوك متعددة الأطراف ذات الصلة بالجريمة السيبرانية وجود أحكام أساسية مشتركة، ولكن يوجد أيضا تباين كبير في المجالات التي تتصدى لها مثل هذه الصكوك

لقد شهد العقد الماضي تطورات هامة في صدور صكوك دولية وإقليمية رامية إلى مكافحة الجريمة السيبرانية، بيد أن هناك تباينا كبيرا في النشأة، والوضع القانوني، والنطاق الجغرافي، والتركيز الموضوعي، والآليات المستخدمة في هذه الصكوك.

ويمكن تحديد خمس "مجموعات" من الصكوك: (1) صكوك تم وضعها في سياق مجلس أوروبا أو الاتحاد الأوروبي، أو مستوحاة منه، (2) صكوك تم وضعها في سياق كومنولث الدول المستقلة أو منظمة شنغهاي

للتعاون، (3) صكوك تم وضعها في السياق الأفريقي، (4) صكوك تم وضعها من قبل جامعة الدول العربية، و(5) صكوك تم وضعها تحت رعاية الأمم المتحدة أو الكيانات المرتبطة بها.

لا تعتبر هذه المجموعات مطلقة، كما أن هناك مجموعة كبيرة موجودة من التقاسم بين الصكوك، ومثال على ذلك، وجود المفاهيم الأساسية الواردة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية أيضا في العديد من الصكوك الأخرى.[1] هيئات الأمم المتحدة، مثل اللجنة الاقتصادية الأفريقية والاتحاد الدولي للاتصالات لديها أيضا عدد من المشاركات عند وضع الصكوك في السياق الأفريقي، ومنها مشروع اتفاقية الاتحاد الأفريقي والقانون النموذجي للمجموعة الإنمائية للجنوب الأفريقي.

صكوك ملزمة	صكوك غير ملزمة
▪ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية (2001) والبرتوكول الإضافي (2003). ▪ اتفاقية مجلس أوروبا بشأن حماية الأطفال من الاستغلال والاعتداء الجنسي (2007) ▪ تشريعات الاتحاد الأوروبي بشأن التجارة الإلكترونية (2000/31/EC)، وبشأن مكافحة الاحتيال وتزييف المدفوعات غير النقدية (2001/413/JHA)، وبشأن البيانات الشخصية بصيغته المعدلة (2002/58/EC)، وبشأن الهجمات ضد نظم المعلومات والمعلومات الشخصية بصيغته النهائية (517/2010) 2005/222/JHA)، وبشأن استغلال الأطفال في المواد الإباحية (2011/92/EU)	▪ القانون النموذجي لدول اتحاد الكومنولث بشأن استخدام الحاسوب في ارتكاب الجرائم (2002) والأدلة الإلكترونية (2002)
▪ اتفاقية كومنولث الدول المستقلة بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية (2001). ▪ اتفاق منظمة شانغهاي للتعاون في ميدان أمن المعلومات على الصعيد الدولي (2009)	
▪ (مشروع) المجموعة الاقتصادية لدول غرب أفريقيا (الإيكواس)، توجيه بشأن مكافحة الجريمة السيبرانية (2009) ▪ (مشروع) اتفاقية الاتحاد الإفريقي لإنشاء إطار قانوني لمساعدة الأمن السيبراني في أفريقيا (2012)	▪ مشروع مجموعة شرق أفريقيا بشأن الإطار القانوني للقوانين السيبرانية (2008) ▪ مشروع الميثاق النموذجي للأمن السيبراني للسوق المشتركة لشرق وجنوب أفريقيا (الكوميسا) (2011) ▪ القانون النموذجي للمجموعة الإنمائية للجنوب الأفريقي بشأن الجرائم الحاسوبية والجريمة السيبرانية (2012)
▪ الاتفاقية العربية بشأن مكافحة جرائم تكنولوجيا المعلومات (2010)	▪ القانون النموذجي للدول العربية بشأن مكافحة جرائم تكنولوجيا المعلومات (2004)
▪ البروتوكول الاختياري لاتفاقية الأمم المتحدة لحقوق الطفل بشأن بيع الأطفال، واستغلالهم في البغاء والمواد الإباحية (2000)	▪ الاتحاد الدولي للاتصالات/الاتحاد الكاريبي/النصوص التشريعية النموذجية لاتحاد الاتصالات الكاريبي بشأن الجريمة السيبرانية، والجريمة الالكترونية والأدلة الالكترونية (2010) ▪ الاتحاد الدولي للاتصالات/أمانة القانون النموذجي لمنطقة المحيط الهادي بشأن الجريمة السيبرانية (2011)

[1] يبين التحليل الوارد في الملحق الثالث المرافق لهذه الدراسة (الأحكام الواردة في الصكوك الدولية والإقليمية) أن العديد من المفاهيم الأساسية المدرجة في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، مثل النفاذ غير المشروع لنظام الحاسوب، والاعتراض غير المشروع للبيانات الحاسوبية، الاختراق غير المشروع لنظام الحاسوب أو البيانات الحاسوبية، التحفظ المعجل على البيانات الحاسوبية والوقت الحقيقي لجمع البيانات الحاسوبية، تعتبر أيضا مدرجة لاحقا في صكوك أخرى.

وقد يكون للصكوك علاقة محددة مباشرة *داخل* إحدى المجموعات، مثل؛ اعتماد القانون النموذجي لدول الكومنولث بشكل وثيق على اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. وإلى جانب ذلك، أدرج مشروع اتفاقية الاتحاد الأفريقي لغة المشروع التوجيهي للجماعة الاقتصادية لدول غرب أفريقيا، بالإضافة إلى ذلك، تظهر اتفاقية كومنولث الدول المستقلة واتفاقية منظمة شنغهاي للتعاون مفاهيم مشتركة تتعلق بأمن المعلومات الحاسوبية.

ويمكن توضيح أوجه التشابه والاختلاف بين الصكوك والمجموعات من خلال المخطط أدناه، مع التركيز على "المركز القانوني"، "والنطاق الجغرافي"، والتركيز الموضوعي"، و"الآليات".

الوضع القانوني

إن أهم سمة يمكن أن يتميز بها أحد الصكوك هي كونه ملزما قانونيا من عدمه. ويشكل عدد من الصكوك، ولاسيما اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، اتفاقية كومنولث الدول المستقلة واتفاقية منظمة شنغهاي للتعاون، والاتفاقية العربية بشأن مكافحة جرائم تكنولوجيا المعلومات، اتفاقيات صريحة بين الدول لترتيب التزامات قانونية متبادلة.[1] وفي هذا الصدد، على سبيل المثال، إذا وافقت الجمعية العامة للاتحاد الأفريقي، فإن مشروع اتفاقية دول الاتحاد الأفريقي يُعرض للتوقيع أو التصديق أو الانضمام، مع دخول الاتفاقية حيز النفاذ في شكل صك ملزم.[2]

الوضع القانوني	النطاق الجغرافي
• ملزم • غير ملزم	• غير مقيد • محدد

التركيز الموضوعي	الآليات
• التجريم (–قائمة الجرائم، –الجرائم الخاصة) • التعاون الدولي والاختصاص القضائي • الصلاحيات الإجرائية • الأمن السيبراني • التجارة الإلكترونية	• ترتيب التزامات • تسليم المطلوبين • المساعدة المتبادلة • وحدات الاتصال

وفيما يتعلق بالصكوك الأخرى، مثل القانون النموذجي لدول اتحاد الكومنولث، ومشروع الميثاق النموذجي للأمن السيبراني للسوق المشتركة لشرق وجنوب أفريقيا (الكوميسا)، والقانون النموذجي للدول العربية بشأن مكافحة جرائم تكنولوجيا المعلومات، والنصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/المجموعة الكاريبية/الاتحاد الكاريبي للاتصالات، فإنها لا تضع التزامات قانونية على الدول. وبالأحرى، قد تمت صياغة هذه

[1] تضع "الاتفاقيات الدولية" سواء كانت عامة أو خاصة، قواعد صريحة معترف بها، ومنها اعتبارها أحد مصادر القانون الدولي، حيث يسري على هذه الاتفاقيات المادة 38 من النظام الأساسي لمحكمة العدل الدولية. وذهبت المادة الثانية من اتفاقية فيينا لقانون المعاهدات إلى تعريف "المعاهدة" بأنها الاتفاق الدولي المعقود بين الدول في صيغة مكتوبة والذي ينظمه القانون الدولي، سواء تضمنته وثيقة واحدة أو وثيقتان متصلتان أو أكثر ومهما كانت تسميته الخاصة.

[2] مشروع اتفاقية الاتحاد الأفريقي، الجزء الرابع، القسم الثاني. أيلول/سبتمبر 2012، الدورة الرابعة العادية لمؤتمر الاتحاد الأفريقي للوزراء المسؤولين عن الاتصالات وتكنولوجيا المعلومات (CITMC-4)، طلب تسليم مشروع اتفاقية الاتحاد الأفريقي إلى لجنة الاتحاد الأفريقي لاعتمادها طبقا للقواعد الإجرائية المعمول بها في الاتحاد الأفريقي. أنظر:

African Union. 2012. *Khartoum Declaration*. AU/CITMC-4/MIN/Decl.(IV)Rev 2, 6 September 2012.

الصكوك لتكون بمثابة توجيه أو "نموذج" لسن أحكام تشريعية وطنية. وبالرغم من ذلك، فقد يكون لدى الصكوك غير الملزمة تأثير هام على المستوى العالمي والإقليمي، وذلك عندما تتجه إرادة الدول إلى مواءمة قوانينها الوطنية مع نُهُج نموذجية.[1] بالإضافة إلى ذلك، فإنه يجوز للدول التي لم تصادق على أحد الصكوك الملزمة أو لم تنضم إليها، بالرغم من ذلك، استعمال هذه الصكوك كتوجيه عند وضع الأحكام التشريعية الوطنية ونتيجة لذلك، قد يكون نطاق أحد الصكوك أكبر من عدد الدول التي قد وقعت أو صادقت أو انضمت إليه.[2]

النطاق الجغرافي

فيما يتعلق بالصكوك الملزمة، يتحدد النطاق الجغرافي عادة وفقا لطبيعة وسياق المنظمة التي وضعت الصك تحت رعايتها. وبالتالي، على سبيل المثال، قامت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بغرض "تعزيز وتدعيم" التعاون بين *الدول العربية*.[3] وبشكل مماثل، جاء في صدر اتفاقية الكومنولث للدول المستقلة تعريف "الأطراف" بأنهم "*الدول الأعضاء في اتحاد دول الكومنولث المستقلة*"،[4] كما نص مشروع اتفاقية الدول الأفريقية على أن تكون الاتفاقية مفتوحة لـ "*الدول الأعضاء في الاتحاد الأفريقي*".[5]

وفيما يتعلق بالعضوية، لا يشترط بالضرورة أن تتزامن عضوية الصك مع العضوية التنظيمية، حيث لا يعتبر كل أعضاء المنظمة من الدول الموقعة على الاتفاقية الأصلية[6]– حيث تخضع الاتفاقية للتصديق أو القبول أو الموافقة[7]– وليست كل الدول الموقعة قد قامت بإيداع هذه الصكوك.[8] فقد تُعرض بعض الصكوك للتوقيع من

[1] لقد استخدمت، على سبيل المثال، عدد من دول اتحاد الكومنولث الأحكام الواردة في القانون النموذجي لدول اتحاد الكومنولث إما منفردا أو بالمشاركة مع اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. أُنظر

Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law. Council of Europe's contribution to the Commonwealth Working Group on Cybercrime.

[2] أبلغ مجلس أوروبا، على سبيل المثال، بالإضافة إلى الدول التي قد صادقت أو وقعت أو تمت دعوتهم للانضمام إلى اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، أنه قد تعامل مع 55 دولة على الأقل في مجال التعاون التقني على أساس الاتفاقية. أُنظر

Seger, A., 2012. The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web.

[3] المادة الأولى من الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات.

[4] اتفاقية دول اتحاد كومنولث الدول المستقلة، التمهيد

[5] مشروع اتفاقية الاتحاد الأفريقي، الجزء الرابع، القسم الثاني، المادة الثانية (د).

[6] تعتبر جزر القمر، جيبوتي ولبنان والصومال من الدول الأعضاء في جامعة الدول العربية ولم يوقعوا على الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات. وبالمثل لم تقم الدول الأعضاء في مجلس أوروبا بالتوقيع على اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، وهم أندورا وموناكو والاتحاد الروسي، وسان مارينو.

[7] نصت المادة 14 من اتفاقية فيينا بشأن قانون المعاهدات على أن " تعبر الدولة عن رضاها الالتزام بالمعاهدة بالتصديق عليها في إحدى الحالات التالية: (أ) إذا نصت المعاهدة على أن التعبير عن الرضا يتم بالتصديق؛ أو (ب) إذا ثبت بطريقة أخرى أن الدول المتفاوضة كانت قد اتفقت على اشتراط التصديق؛ أو (ج) إذا كان ممثل الدولة قد وقع المعاهدة بشرط التصديق؛ أو (د) إذا بدت نية الدولة المعنية من وثيقة تفويض ممثلها أن يكون توقيعها مشروطا بالتصديق على المعاهدة، أو عبرت الدولة عن مثل هذه النية أثناء المفاوضات. وفي هذا الصدد، نصت صراحة كل من الاتفاقية العربية لمكافحة الجرائم المتعلقة بتكنولوجيا المعلومات واتفاقية مجلس أوروبا بشأن الجريمة السيبرانية أن الاتفاقية خاضعة للتصديق أو القبول أو الموافقة. كما تقتضي اتفاقية كومنولث الدول المستقلة واتفاقية منظمة شنغهاي للتعاون بأن يقوم الأطراف بإيداع إشعار اكتمال الإجراءات الداخلية المطلوبة لدخول الاتفاقية حيز النفاذ. وبالمثل، فإن مشروع اتفاقية الاتحاد الأوروبي عرض الاتفاقية للتوقيع أو التصديق أو الانضمام. وللاستعراض اتفاقية فيينا لقانون المعاهدات بشكل عام، أُنظر:

Shaw, M.N., 2007. *International Law*. 6th ed. Cambridge: Cambridge University Press.

[8] لم تودع بعد كل من جمهورية التشيك، اليونان، أيرلندا، ليختنشتاين، لوكسمبورغ، بولندا، السويد وتركيا صكوك التصديق أو القبول أو الموافقة فيما يتعلق باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

خارج عضوية المنظمة تحت رعاية من قام بوضع الصك، فعلى سبيل المثال، قد فتحت اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية التوقيع للدول الأعضاء في مجلس أوروبا و"*للدول غير الأعضاء الذين شاركوا في صياغتها*".[1]

تعتبر الدول المؤسسة بمثابة الدول صاحبة الاختصاص الأصيل التي تتحكم في دخول دول جديدة تطلب الانضمام، ويتم ذلك غالبا طبقا للقواعد المنصوص عليها في الاتفاق الأولي.[2] وجرَت العادة، أن "تفتح" المعاهدات أمام أي دولة راغبة في الانضمام، وذلك من خلال الإفصاح عن نيتها بالالتزام بالشروط والأحكام الواردة في المعاهدة الموجودة، كما قد تكون المعاهدة "شبة مفتوحة" حيث يمكن توسيع نطاقها بالموافقة من قبل أغلبية الدول الموقعة و/أو الدول المتعاقدة، بالإضافة إلى ذلك، قد تكون المعاهدة "مغلقة" حيث يتطلب توسيع نطاقها موافقة بالإجماع من الدول الموقعة و/ أو الدول المتعاقدة.[3]

وفيما يتعلق باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، فإنه يجوز للجنة وزراء مجلس أوروبا بعد التشاور والحصول على موافقة بالإجماع من الدول المتعاقدة في الاتفاقية أن "*تدعو أي دولة ليست عضوا في المجلس ولم تشارك في صياغة الاتفاقية بأن تنضم إلى الاتفاقية*".[4] وعلى نحو مماثل، تعتبر اتفاقية كومنولث الدول المستقلة "*مفتوحة لانضمام أي دولة من الدول الأخرى راغبة في الالتزام بالأحكام الواردة في الاتفاقية، بشرط موافقة كل الأطراف*".[5] كما تنص أيضا اتفاقية منظمة شنغهاي للتعاون على أنها "*مفتوحة لانضمام أي دولة تشارك في الأهداف والمبادئ الواردة في الاتفاقية*".[6] فمن المستقر أن الصكوك التي وضعت تحت رعاية الأمم المتحدة تتمتع بنطاق جغرافي أوسع بشكل مطلق. فعلى سبيل المثال؛ اتفاقية حقوق الطفل وبرتوكولها الاختياري بشأن بيع الأطفال، واستغلال الأطفال في البغاء، وفي المواد الإباحية، مفتوحة "*لانضمام أي دولة*".[7]

---

[1] اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 36(1). قامت كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية وهم من الدول غير الأعضاء، بالتوقيع في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

[2] نصت المادة 15 من اتفاقية فيينا بشأن قانون المعاهدات على أن: " تعبر الدولة عن رضاها الالتزام بالمعاهدة بالانضمام إليها في إحدى الحالات التالية: (أ) إذا نصت المعاهدة على أن التعبير عن الرضا يتم بالانضمام؛ أو (ب) إذا ثبت بطريقة أخرى أن الدول المتفاوضة كانت قد اتفقت على أن التعبير عن الرضا يتم بالانضمام؛ أو (ج) إذا اتفقت جميع الأطراف فيما بعد على أن التعبير عن الرضا يتم بالانضمام".

[3] Malone, L.A., 2008. *International Law*. New York: Aspen

[4] اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المادة 37 (1). اقترحت اللجنة المعنية باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية بتعديل الإجراءات الواردة في المادة 37 (1) كما أبدت ذلك أيضا اللجنة الأوروبية المعنية بمشاكل الجريمة. ويعتبر كلا المقترحين في الوقت الحالي قيد الاستعراض من قبل فريق المقررين للمجلس الأوروبي المعني بالتعاون القانوني. أنظر: اللجنة المعنية باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية 2012. معايير وإجراءات الانضمام إلى اتفاقية بودابست بشأن جرائم الإنترنت–تم التحديث (2012) 12 هـ. 28 آيار/مايو 2012.

[5] المادة (17) من اتفاقية كومنولث الدول المستقلة

[6] المادة (12) من اتفاقية منظمة شنغهاي للتعاون

[7] المادة 48 من اتفاقية الأمم المتحدة لحقوق الطفل، الأمم المتحدة (اتفاقية حقوق الطفل–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن اشتراك الأطفال في النزعات المسلحة–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء والمواد الإباحية) المادة 13. "الدولة" ذات مفهوم واسع في هذا المحتوى ولا يقتصر على الدول الأعضاء في الأمم المتحدة، فعلى سبيل المثال الكرسي الرسولي بوصفها دولة، قد وقعت وصادق على الاتفاقية المعنية بحقوق الطفل و(اتفاقية حقوق الطفل–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن اشتراك الأطفال في النزاعات المسلحة–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء والمواد الإباحية). أُنظر:

http://treaties.un.org/Pages/Treaties.aspx?id=4&subid=A&lang=en

وتتمتع الدول المؤسسة بميزة التأثير على محتوى المعاهدة، لَكِنْ قد تواجه بعض الأعباء المتعلقة بصياغة المعاهدة وعمليات التفاوض بشأنها. ويجنب الانضمام اللاحق لمعاهدة تحمل هذه الأعباء، بيد أن ذلك يحد من فرص التفاوض بشأن المحتوى والالتزامات الواردة فيها. وبقدر ما تبرم المعاهدات غالبا من قبل الدول بنفس الاتجاهات، إلا أن المعاهدات قد لا تكون مقبولة للدول التي لم تشارك في المفاوضات، حتى في حالة إذا ما تركت المعاهدة مفتوحة للانضمام.[1]

عادة يعترف بالمعاهدة متعددة الأطراف من خلال نظام التحفّظات الذي يجوز إبداؤه في وقت التوقيع أو التصديق أو الانضمام.[2] وفي هذا الصدد، تجيز اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية إبداء تحفظات محددة بشأن مواد معينة واردة في الاتفاقية، على الرغم من أنه لا يجيز إبداء أي تحفّظات أخرى.[3] وعلى نحو متطابق، تجيز الاتفاقية العربية لمكافحة جرائم المعلومات إبداء تحفظات محددة، وتحظر فقط التحفظات التي "*تنطوي على انتهاك لنصوص الاتفاقية أو خروجا عن أهدافها*"،[4] في حين أن اتفاقية كومنولث الدول المستقلة لم تتعرض لمسألة التحفّظات،[5] إلا أن إحدى الدول الأعضاء، على الأقل، أبدت تحفظا واحدا.[6] تسمح اتفاقية الاتحاد الأفريقي بإبداء تحفّظات بشأن "*واحدة أو عدة من الأحكام*" *التي لا تتعارض مع أهداف ومقاصد الاتفاقية*".[7] وذلك، في حالة إذا أعتمدت الاتفاقية في شكلها الحالي.

فعلى الصعيد العالمي، قد وقعت و/أو صادقت 82 دولة على أحد الصكوك الملزمة المعنية بمكافحة الجريمة السيبرانية،[8] وتعتبر بعض الدول في هذه الاتفاقية أعضاء في أكثر من اتفاقية أخرى. بالرغم من احتمالية المشاركة من خارج السياق التنظيمي الأصلي أو عملية الصياغة للاتفاقية، إلا أن الشكل 3-6[9] يُظهر أنه حتى الآن لا يوجد صك واحد قد حظي بتوقيعات أو تصديقات/انضمامات مع الامتداد الجغرافي العالمي، وذلك بغض

---

[1] Parisi, F., Fon, V., 2009. The Formation of International Treaties. *In: The Economics of Lawmaking.* Oxford: Oxford Scholarship Online

[2] ويتناول الجزء الثاني من اتفاقية فيينا لقانون المعاهدات المسائل المتعلقة بإبداء التحفظات والاعتراض عليها والآثار القانونية المترتبة عليها، والآثار القانونية المترتبة على إبداء الاعتراض على التحفظات، كذلك يتناول الجزء الثاني؛ عملية سحب التحفظات والاعتراضات، والإجراءات المتعلقة بإبداء التحفظات. وبصفة عامة لا يقبل أي من التحفظات التي تتعارض مع أغراض المعاهدة وأهدافها.

[3] المادة 42 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

[4] المادة 6، الفصل الخامس من الاتفاقية العربية لمكافحة جرائم المعلومات.

[5] بموجب المادة 24 من اتفاقية فيينا لقانون المعاهدات، فإن الموقف الافتراضي يتجسد في جواز إبداء التحفظات من جانب أي دولة ما لم يحظر على وجه الخصوص من جانب المعاهدة أو عندما تنص المعاهدة على تحفظات محددة فقط، أو إذا كان التحفظ يتنافى مع أهداف وأغراض من المعاهدة.

[6] تحفظت أوكرانيا في إطار البند 5 من جدول من جدول أعمال اجتماع مجلس رؤساء الدول الأعضاء في رابطة الدول المستقلة، تحت عنوان "اتفاق بشأن التعاون في مجال مكافحة الجرائم المتصلة بالمعلومات الحاسوبية" 1 حزيران/يونيو 2001.

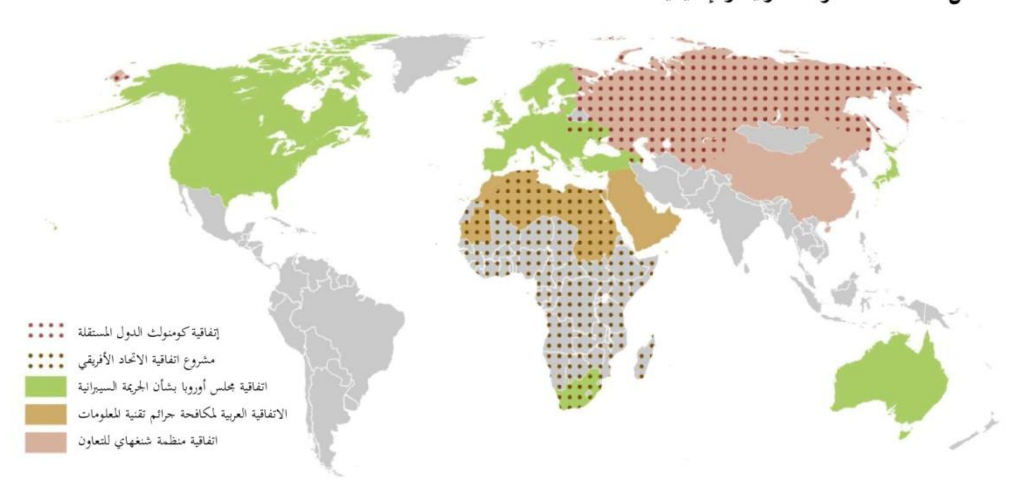
[7] مشروع اتفاقية الاتحاد الأفريقي، الجزء الرابع، القسم الثاني، المادة 3(هـ).

[8] التوقيع أو التصديق على اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، الاتفاقية العربية بشأن مكافحة جرائم المعلومات اتفاقية كومنولث الدول المستقلة واتفاقية منظمة شنغهاي للتعاون.

[9] تظهر الخريطة كل الدول التي إما وقعت أو صادق أو انضمت إلى اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، الاتفاقية العربية بشأن مكافحة جرائم المعلومات اتفاقية كومنولث الدول المستقلة واتفاقية منظمة شنغهاي للتعاون. وللمرجعية، فإن الخريطة أيضا تُبَيّن عضوية الاتحاد الأفريقي، وهو ما يمثل مجموع الأعضاء المحتملين للمشروع اتفاقية الاتحاد الأفريقي، إذا وافقت الدول أو عرضت الاتفاقية للتوقيع والتصديق أو الانضمام.

النظر عن صكوك الأمم المتحدة المعنية باتفاقية حقوق الطفل – البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن اشتراك الأطفال في النزعات المسلحة – البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء والمواد الإباحية.[1] وتمثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية أكبر عدد من التوقيعات أو التصديقات/الانضمامات (48 دولة)، بما فيها عدد خمس دول ليست أعضاء في مجلس أوروبا،[2] بينما لدى الصكوك الأخرى نطاق جغرافي أصغر، فعلى سبيل المثال: الاتفاقية العربية بشأن مكافحة جرائم المعلومات (18 دولة أو إقليم)، اتفاقية كومنولث الدول المستقلة (10 دول)، واتفاقية منظمة شنغهاي للتعاون (6 دول)، أما بالنسبة لمشروع اتفاقية الاتحاد الأفريقي، قد يصل عدد الدول فيه إلى 54 دولة أو إقليم في حالة إذا وقعت أو صادقت جميع الدول الأعضاء في الاتحاد الأفريقي على مشروع الاتفاقية.

الشكل 3–6: الصكوك الدولية والإقليمية



وختاما، فإن الصورة العالمية تعد بمثابة أحد درجات التقسيم في عضوية الصكوك الدولية والإقليمية المتعلقة بالجريمة السيبرانية، بيد أن النموذج الإقليمي في هذا الصدد يتسم بالوضوح بشكل خاص. وفي حين تستفيد دول في بعض أجزاء من العالم من عضوية الصكوك الملزمة المعنية بمكافحة الجريمة السيبرانية – بما في ذلك عضوية بعض الدول في أكثر من صك – إلا أن هناك مناطق أخرى لا تشارك في أي إطار ملزم.

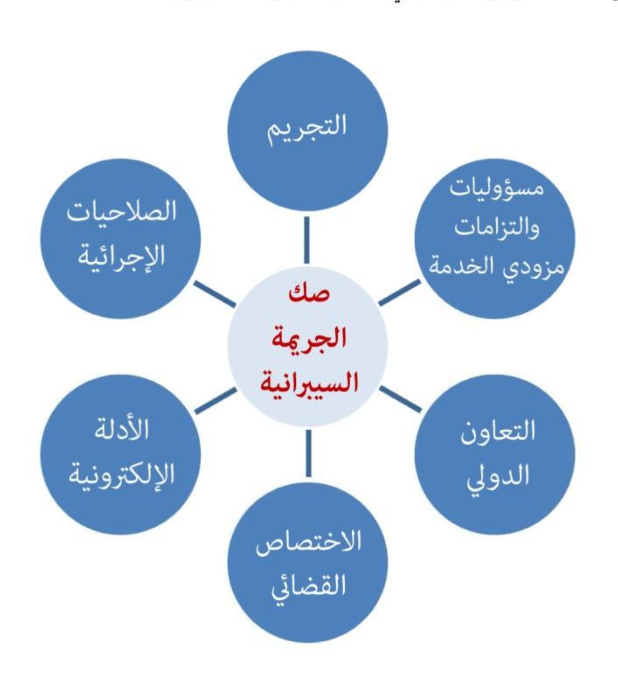
[1] عدد 176 دولة أو إقليما قد وقعت أو صادقت أو انضمت إلى صكوك الأمم المتحدة المعنية باتفاقية حقوق الطفل–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن اشتراك الأطفال في النزعات المسلحة–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء والمواد الإباحية

[2] بالإضافة إلى ذلك، قد وجهت الدعوة لثمانية بلدان أخرى (الأرجنتين، تشيلي، كوستاريكا، جمهورية الدومينيكان، المكسيك، بنما، الفلبين، والسنغال) إلى الانضمام إلى اتفاقية مجلس أوروبا وفقا لأحكام المادة 37، حيث وسع انضمام هذه الدول للاتفاقية من نطاقها الجغرافي بكثير.

التركيز الموضوعي

بالإضافة إلى الاختلافات في النطاق الجغرافي، فإن الصكوك الدولية والإقليمية، إلى جانب التشريعات الوطنية، تُظهر أيضا اختلافات في التركيز الموضوعي، حيث ينبثق العديد من هذه الاختلافات من الهدف الأساسي من الصك. فبعض الصكوك، مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والقانون النموذجي لاتحاد دول الكومنولث، والاتفاقية العربية بشأن مكافحة جرائم المعلومات، واتفاقية كومنولث الدول المستقلة تهدف بشكل خاص إلى توفير إطار العدالة الجنائية لمكافحة أشكال الجريمة السيبرانية. بيد أن الصكوك الأخرى مثل اتفاقية منظمة شنغهاي للتعاون ومشروع اتفاقية الاتحاد الأفريقي تتخذ نهجا أوسع نطاقا حيث تعتبر الجريمة السيبرانية بمثابة الهدف الوحيد، فاتفاقية منظمة شنغهاي للتعاون، على سبيل المثال، تتناول التعاون في الأمور المتلعقة بالجريمة السيبرانية في سياق أمن المعلومات على الصعيد الدولي، بما في ذلك المعلومات بشأن الحروب والإرهاب والتهديدات التي تتعرض لها البنية التحتية للمعلومات العالمية والوطنية.[1] أما فيما يتعلق بمشروع اتفاقية الاتحاد الأفريقي، فإنها تقوم على نهج الأمن السيبراني الذي يتضمن تنظيم المعاملات الإلكترونية، وحماية البيانات الشخصية، وتعزيز الأمن السيبراني، والحوكمة الإلكترونية ومكافحة الجريمة السيبرانية.[2]

الشكل 3–7: التركيز الموضوعي لصكوك الجريمة السيبرانية



تؤثر هذه الاختلافات بشكل كبير على الوسيلة التي تصاغ بها الجريمة السيبرانية أثناء التَجَاوُب القانوني الدولي أو الإقليمي، ويرجع ذلك إلى أن اتساع نطاقها يركز على أمن المعلومات على الصعيد الدولي، فعلى سبيل المثال، لم تضع اتفاقية منظمة شنغهاي للتعاون أفعالا سيبرانية محددة يجب أن تجرّم، وربما يرجع ذلك إلى تركيزها على الأمن السيبراني ككل، بدلا من التركيز على العدالة الجنائية بشكل خاص. وعلى نحو مماثل، لم يسع مشروع

[1] تتضمن المادة الثانية من اتفاقية منظمة شنغهاي للتعاون، الجريمة السيبرانية باعتبارها "تهديدا كبيرا" لأمن المعلومات على الصعيد الدولي. وعرف الملحق 1 من الاتفاقية "الجريمة السيبرانية بأنها "استعمال موارد المعلومات في أغراض غير مشروعة و(أو) تأثير ذلك عليها في الفضاء المعلوماتي"

[2] وحدد الجزء الثالث من مشروع اتفاقية الاتحاد الأفريقي الجريمة السيبرانية بأنها "تعزيز الأمن السيبراني ومكافحة الجريمة السيبرانية. أما الجزء الأول والثاني من نفس الاتفاقية، فقد تناول على التوالي: "المعاملات الإلكترونية" و"حماية البيانات الشخصية".

الاتحاد الأفريقي في الوقت الحالي إلى إنشاء آليات للتعاون الدولي في المسائل الجنائية ذات الصلة بالجريمة السيبرانية.

وطبقا لمنظور العدالة الجنائية ومنع الجريمة، توجد ستة مجالات رئيسية يمكن الاستفادة منها كتوجيه إرشادي ملزم أو غير ملزم على الصعيد الدولي أو الإقليمي: (1) التجريم، و(2) الصلاحية الإجرائية للهيئات المكلفة بإنفاذ القانون، و(3) الإجراءات المتعلقة بالأدلة الإلكترونية، و(4) الولاية القضائية للدولة في المسائل الجنائية المتعلقة بالجريمة السيبرانية، و(5) التعاون الدولي في المسائل الجنائية المتعلقة بالجريمة السيبرانية، و(6) مسؤولية مقدمي الخدمات.

فمن المستقر أنه يمكن تحليل كل مجال من المجالات التي تشكل فَحْوَى الصكوك الدولية والإقليمية – وفي الواقع، القوانين الوطنية أيضا – على ثلاثة مستويات: (1) وجود الأحكام ذات الصلة في كل مجال، (2) تناول الأحكام داخل كل مجال، (3) محتوى الأحكام. ويتناول هذا القسم المستوى الأول والثاني، أما المستوى الثالث فيتم تناوله في الفصل الرابع (التجريم) والفصل الخامس (التحقيقات وإنفاذ القانون).

وفيما يتعلق بوجود الأحكام ذات الصلة، فقد حددت الصكوك الدولية والإقليمية الملزمة وغير الملزمة ماهية المجالات الستة المختلفة؛ ومنها الأحكام المتعلقة بالتجريم، والأحكام المتعلقة بالصلاحيات الإجرائية، والأحكام المتعلقة بالولاية القضائية، والأحكام المتعلقة بالتعاون الدولي والتي توجد عموما في عدد من الصكوك الملزمة. وعلى النقيض من ذلك، فإن الصكوك غير الملزمة تتناول عادة الأحكام المتعلقة بالأدلة الإلكترونية ومسؤوليات مقدمي خدمة الإنترنت، مثل؛ القانون النموذجي لدول اتحاد الكومنولث، ومشروع الميثاق النموذجي للسوق المشتركة لشرقي وجنوبي أفريقيا (الكوميسا)، والنصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات.[1] ويتضمن فقط المشروع التوجيهي للجماعة الاقتصادية لدول غرب أفريقيا (إيكواس) ومشروع اتفاقية الاتحاد الأفريقي (من المتَصَوّر أن تكون ملزما) أحكاما تتعلق بالأدلة الإلكترونية.[2] وعلى نحو مماثل، فإن تشريعات

الشكل 3–8: هيكل الصكوك الدولية والإقليمية



[1] أنظر الجدول الخاص بـ "الأدلة الإلكترونية" و"مسؤوليات والتزامات مقدمي خدمة الإنترنت"، الملحق الثالث المرافق لهذه الدراسة

[2] أنظر المادة 34 من المشروع التوجيهي للجماعة الاقتصادية لدول غرب أفريقيا، والمادة 24/ط من مشروع اتفاقية الاتحاد الأفريقي.

الاتحاد الأوروبي تتناول مسألة مقدمي خدمة الإنترنت من حيث مسؤولياتهم والتزاماتهم على المستوى الإقليمي أو الدولي.[1]

تُظهر أيضا الصكوك مجموعة من النُهُج داخل المجالات المعنية بالتجريم، والصلاحيات الإجرائية لإنفاذ القانون، والتعاون الدولي، ويوضح الشكل 3-8 التوزيع النسبي لعدد المواد الواردة في خمسة صكوك دولية أو إقليمية تتناول كل مجال على حدة. وجدير بالذكر، أن هناك صكوكا تتناول كافة المجالات الأربعة، ومن هذه الصكوك اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بيد أن مشروع اتفاقية الاتحاد الأفريقي يركز بشكل كبير على التجريم مع إدراج بعض من الصلاحيات الإجرائية. أما فيما يتعلق باتفاقية كومنولث الدول المستقلة، فإنها تتضمن عددا قليلا من المواد المعنية بالتعاون الدولي والتجريم. هذا، ولم تتناول اتفاقية منظمة شنغهاي للتعاون من المجالات الأربعة سوى المواد المتعلقة فقط بالتعاون الدولي.

وفيما يتعلق بالمستوى الثاني، فإن تناول الأحكام ذات الصلة بالصكوك يختلف أيضا بشكل كبير، ويتضمن الملحق الثالث المرافق لهذه الدراسة تحليلا كاملا لتغطية المواد لكل مجال من المجالات الستة الرئيسية الواردة في الصك. ويبين التحليل مدى التنوع في السلوك الذي تجرمه الصكوك واتساع نطاق الصلاحيات الإجرائية لإنفاذ القانون بالإضافة إلى تَمَدَّد النُهُج التي تتناول الولاية القضائية والتعاون الدولي.

ويُبيّن الملحق الثالث أيضا أنه بالرغم من الاختلافات الجوهرية الموجودة إلا أن العديد من الصكوك تشترك في "أحكام أساسية" معينة، ومنها على وجه الخصوص: تجريم الأفعال المرتكبة ضد السرية، والنزاهة، وتوافر بيانات حاسوبية أو نظم حاسوب، وكذلك الصلاحيات الإجرائية التي تتضمن التفتيش والمصادرة والأوامر الخاصة بالبيانات الحاسوبية، والوقت الحقيقي لجمع البيانات الحاسوبية، والتحفظ على البيانات الحاسوبية، والالتزامات العامة بشأن التعاون في إجراء التحقيقات المنوطة بالمسائل الجنائية للجريمة السيبرانية. ويوجز الجدول التالي بعضا من النتائج الرئيسية المترتبة على إجراء التحليل الكامل، والوارد في الملحق الثالث.

التجريم	• تتضمن معظم الصكوك قائمة عريضة من الجرائم، حيث تركز الصكوك الأخرى على مجال محدود من الجرائم النوعية، مثل الصكوك التي تركز على حماية الطفل، وتلك التي تتناول جرائم استغلال الطفل في المواد الإباحية • من الأفعال الأكثر تجريما تلك المرتكبة ضد السرية، والنزاهة، وتوافر بيانات حاسوبية أو نظم حاسوب، تليها الأفعال المتعلقة باستخدام الحاسوب في الاحتيال والتزوير، واستخدام الحاسوب في إنتاج أو توزيع أو مواد إباحية عن الأطفال • بالإضافة إلى الأفعال المحددة في الفصل الأول من هذه الدراسة والواردة في القسم المعني ب"توصيف الجريمة السيبرانية"، حيث تجرم أيضا بعض الصكوك نطاقا عريضا من

[1] أنظر على سبيل المثال التوجيهي الصادر عن الاتحاد الأوروبي بشأن التجارة الإلكترونية، المواد من 12 إلى 15.

	الأفعال، منها استخدام الحاسوب في ارتكاب أفعال ضد النظام العام والآداب العامة أو الأمن القومي • نصت بعض الصكوك على أن ارتكاب جرائم تقليدية باستخدام وسائل تتعلق بنظام حاسوبي، يعتبر ظرفا مشددا للعقوبة
الصلاحيات الإجرائية	• يعتبر التفتيش والمصادرة وأوامر بيانات الحاسوب المخزنة والمعلومات المشتركة، الوقت الحقيقي لجمع البيانات الحاسوبية، الأمر العاجل بالتحفظ على البيانات الحاسوبية، من الصلاحيات الإجرائية الشائعة في الصكوك • النفاذ عبر الحدود إلى نظم أو بيانات حاسوبية
الأدلة الإلكترونية	• تعتبر الصكوك (وبخاصة غير الملزمة) التي تتصدى للأدلة الإلكترونية قليلة، حيث تتناول مجالات منها؛ الشروط العامة لقبول الأدلة الإلكترونية، صِحّة عبء الإثبات، ومبدأ أفضل دليل، وافتراض السلامة، ومعايير التحفظ على الأدلة
الولاية القضائية	• تتضمن تقريبا كافة الصكوك مبدأ الإقليمية ومبدأ الجنسية (حيث توجد ازدواجية التجريم) كأساس للاختصاص القضائي • لم يتم العثور في الصكوك الأخرى على أسس أخرى يقوم عليها الاختصاص القضائي، بما في ذلك مبدأ الأعمال الموجهة إلى نظام الحاسوب أو البيانات الحاسوبية الواقعة في إقليم ومصالح إحدى الدول • ينص صكان على توجيهات بشأن تحديد محل وقوع إحدى الجرائم السيبرانية
التعاون الدولي	• توفر الصكوك التي تتناول التعاون الدولي على نطاق أوسع، آليات للمساعدة القانونية المتبادلة وتسليم المجرمين المطلوبين، أو تركز بطريقة مختصرة على المبادئ العامة للتعاون • يتوخى عدد من الصكوك إنشاء وحدات اتصال أو شبكة الـ (7/24)
مقدمو الخدمة	• يتناول العدد المحدود من الصكوك، التي تغطي مسؤولية مقدمي خدمات الإنترنت، مجالات تشتمل على رقابة الالتزامات، الدعم التطوعي للمعلومات، تسجيل الإخطارات، علاوة على التزاماته بشأن النفاذ والتخزين المؤقت والاستضافة ووصلات الإحالة الإلكترونية

الآليات

تتعلق آليات التعاون الدولي بالصكوك الدولية والإقليمية الملزمة بصفة خاصة، ويرجع ذلك إلى قدرة هذه الصكوك على منح التزام قانوني دولي واضح أو صلاحية ما للتعاون بين الدول الأطراف. وإلى جانب الالتزامات العامة للتعاون،[1] فإن عددا من الصكوك، ولاسيما اتفاقية كومنولث الدول المستقلة واتفاقية مجلس أوروبا بشأن

[1] أنظر على سبيل المثال، المادة 23 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية والتي تنص على أن: "يتعين على الدول الأطراف أن تتعاون مع بعضها البعض طبقا للأحكام الواردة في هذا الفصل، ومن خلال تطبيق الصكوك الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية، والموافقة على الترتيبات على أساس التشريعات

الجريمة السيبرانية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ترسي آليات مُعَيّنة للتعاون. ويمكن التعويل على الاتفاقية ذاتها – من هذه الاتفاقيات الثلاثة – كأساس لطلبات المساعدة من إحدى الدول الطرف إلى أخرى.[1] وعلى هذا النحو؛ وبدون الإخلال بالشروط المنصوص عليها في القانون الوطني أو المعاهدات الأخرى المعنية بالمساعدة القانونية المتبادلة، فإن الاتفاقية قد تعرض الأسباب التي يجوز لأي من الدول بموجبها رفض طلب المساعدة.[2] وتستخدم اتفاقية كومنولث الدول المستقلة المنهج القائم على تحديد نوع المساعدة التي قد تُطلب بعبارات عامة إلى حد ما.[3] وجدير بالذكر في هذا الصدد، بأنه إلى جانب الالتزامات العامة الواردة في كل من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية والاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتقديم المساعدة القانونية على أوسع نطاق ممكن لأغراض التحقيقات أو الإجراءات، فإنهما أيضا تتضمنان أشكالا خاصة من المساعدة، مثل؛ التحفظ العاجل على البيانات الحاسوبية المخزنة، والكشف المعجل عن حركة مرور البيانات المتحفظ عليها، والوصول إلى البيانات الحاسوبية المخزنة، والوقت الحقيقي لجمع حركة مرور البيانات، واعتراض بيانات المحتوى.[4]

وأخيرا، يرسخ عدد من الصكوك فكرة وجود سجلات للسلطات المختصة لأغراض تسليم المجرمين وطلبات المساعدة القانونية المتبادلة،[5] وإجراءات تقديم المساعدة العاجلة،[6] ووحدات الاتصال لتوفير قنوات للتواصل على مدار 24 ساعة يوميا.[7]

الموحدة أو المتَبَادَلة، والقوانين المحلية على أوسع نطاق ممكن لأغراض التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية ذات الصلة بأنظمة الحاسوب أو البيانات، أو لجمع الأدلة في شكل إلكتروني من جريمة جنائية".

[1] أنظر على سبيل المثال، المادة 27 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية والتي تنص على أن: "في حالة عدم وجود معاهدة بشأن المساعدة المتبادلة أو ترتيبات على أساس التشريعات الموحدة أو المتَبَادَلة سارية بين الدولة الطالبة والدولة الموجه لها الطلب، فإن الأحكام الواردة في الفقرات من 2 حتى 9 من هذه المادة تسري في هذه الحالة". كما تنص المادة 34 من الاتفاقية العربية لمكافحة جرائم المعلومات على أن: "تسري الفقرتان 2 حتى 9 من هذه المادة في حالة عدم وجود معاهدة بشأن التعاون والمساعدة المتبادلة أو اتفاقية قائمة على أساس التشريعات المعمول بها بين الدول الأطراف الطالبة المساعدة وتلك التي طُلب منها تقديم المساعدة". وتنص المادة 6 من اتفاقية كومنولث الدول المستقلة على أنه: يتعين أن يكون التعاون في إطار هذه الاتفاقية على أساس طلبات المساعدة التي أعدتها السلطات المختصة للأطراف".

[2] أنظر على سبيل المثال الفقرة 4 من المادة 27 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والمادة 35 من الاتفاقية العربية لمكافحة جرائم المعلومات، حيث تنص كلاهما على أنه يجوز رفض طلب المساعدة إذا كان الطلب يتعلق بجرائم سياسية أو تعتبر الدول المطلوب منها تقديم المساعدة أن الطلب يمس بسيادتها أو أمنها أو نظامها العام أو مصالحها الأساسية أو الجوهرية الأخرى.

[3] تتضمن على سبيل المثال المادة 5 من اتفاقية كومنولث الدول المستقلة؛ تبادل المعلومات بشأن الجرائم ذات الصلة بالمعلومات الحاسوبية التي تعتبر في طور الإعداد أو قد ارتكبت، وتنفيذ طلبات المساعدة لأغراض التحقيق والإجراءات طبقا للصكوك الدولية المعنية بالمساعدة القانونية المتبادلة، وتخطيط وتنفيذ الأنشطة والعمليات التنسيقية لمنع الجرائم ذات الصلة بالمعلومات الحاسوبية بالإضافة إلى الكشف عنها وكبحها وإظهارها والتحقيق فيها.

[4] أنظر المواد 29، 30، 31، 33، و34 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والمواد 37 –39، 41 و42 من الاتفاقية العربية لمكافحة جرائم المعلومات.

[5] أنظر الفقرة 7 من المادة 24، والفقرة 2 من المادة 27 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والمادة 4 من اتفاقية كومنولث الدول المستقلة، فقرة 7 من المادة 31، وفقرة 2 من المادة 34 من الاتفاقية العربية لمكافحة جرائم المعلومات.

[6] أنظر الفقرة 3 من المادة 31 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والفقرة 2 من المادة 6 من اتفاقية كومنولث الدول المستقلة، الفقرة 8 من المادة 34 من الاتفاقية العربية لمكافحة جرائم المعلومات.

[7] أنظر المادة 35 من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والمادة 43 من الاتفاقية العربية لمكافحة جرائم المعلومات.

4-3 تنفيذ الصكوك متعددة الأطراف على الصعيد الوطني

الاستنتاجات الرئيسية:

- إلى جانب العضوية الرسمية والتنفيذ، فإن الصكوك متعددة الأطراف والمنوط بها مكافحة الجريمة السيبرانية ذات تأثير على القوانين الوطنية بشكل غير مباشر، وذلك من خلال استعمالها كنموذج من قبل الدول غير الأطراف، أو عن طريق تأثير تشريعات الدول الأطراف على الدول الأخرى
- تتوافق عضوية الصكوك متعددة الأطراف والمنوط بها مكافحة الجريمة السيبرانية مع التصور بزيادة كفاية القانون الجنائي الوطني والقانون الإجرائي بشكل كاف، مما يشير إلى أن الأحكام المتعددة حاليا في هذه المجالات تعتبر فعّالة بشكل عام
- وقد يعزى عدم الاتساق على المستوى الدولي وتنوّع القوانين الوطنية، من حيث تجريم الأفعال التي تعتبر جرائم سيبرانية والأسس التي تقوم عليها الولاية القضائية وآليات التعاون، إلى وجود صكوك متعددة بشأن الجريمة السيبرانية لها نطاق مواضيعي وجغرافي مختلف

قد يشكل الأسلوب المتبع لدمج الصكوك الدولية والإقليمية في إطار القانون الوطني، فضلا عن فعالية التطبيق وتنفيذ القواعد الجديدة عاملا قطعيا في نجاح عملية المواءمة،[1] أو غير ذلك من الأمور ذات الصلة. وقد تضطلع الدول بتفسير أو تنفيذ الأحكام الواردة في الصكوك الدولية بطرائق مختلفة، مما يؤدي إلى زيادة التباعد بين الدول، حيث لا يمثل ذلك التباعد مشكلة في حد ذاته، فمن الثابت أن الدول دائما لا تضطلع بتنفيذ الأطر الدولية بنفس الأسلوب تماما، وذلك بسبب اختلاف التقاليد القانونية والقيود الموجودة على المستوى الوطني.[2] وفي نفس الوقت، من ناحية ثانية، يتجسد الهدف من التنفيذ في توفير درجة محددة من التوافق بين التشريعات الوطنية والأطر الدولية.

التنفيذ الرأسي (المباشر)

يتبع التنفيذ "المباشر" للمعاهدة متعددة الأطراف التوقيع والتصديق على المعاهدة أو الانضمام لها. ويتعين أن يضطلع موظفو الدولة أو الأفراد بتطبيق معظم القواعد القانونية لكي تصبح نافذة في إطار النظم القانونية المحلية. ويجوز للدول تحقيق ذلك إما من خلال "الدمج المستمر" للقواعد الدولية مع القانون الوطني (غالبا

[1] Miquelon-Weismann, M. F., 2005. The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? *John Marshall Journal of Computer & Information Law*, 23(2):329-61.

[2] See Klip, A., Nelken, D., 2002. Changing Legal Cultures. *In*: Likosky, M. (ed.) *Transnational Legal Processes*. London: Butterworths; Graziadei, M., 2009. Legal Transplants and the Frontiers of Legal Knowledge. *Theoretical Inquiries in Law*, 10(2): 723-743

ما يرتبط ذلك مع ما يسمى بالأنظمة "الأحادية")، أو عن طريق "دمج التشريع" (في أنظمة "ثنائية")، حيث تصبح القواعد الدولية جزءا لا يتجزأ من النظام القانوني الوطني، وذلك فقط عند سن التشريع الوطني ذو الصلة.[1]

غالبا ما يتطلب إدراج الأحكام الواردة في الصك المعني بالجريمة السيبرانية في القانون الوطني تعديل التشريع، مثل القانون الجنائي وقانون الإجراءات الجنائية، وذلك لتقنين الجرائم الجديدة الخاصة أو تعديل القائمة.

وغني عن البيان، أن نتيجة إدراج القواعد الدولية في القانون الوطني قد تختلف إلى حد كبير من دول طرف إلى دولة طرف أخرى. فإحدى التأثيرات الخاصة لتنفيذ أحد الصكوك الدولية على النظام القانوني الوطني لإحدى الدول، قد لا يحدث في دول أخرى،[2] على سبيل المثال. يوضح بشكل جيد تقييم تنفيذ قرار الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات[3] التحديات التي تَعَرّضَ لها في مواءمة تشريعات مكافحة الجريمة السيبرانية، حتى في سياق إطار ملزم، ودول اعتادت على تنفيذ قانون مُتَخطِّي الحدود الوطنية.[4] وعلى النحو المبين في الجدول، أظهر تقييم عملية التنفيذ تباينات كبيرة في الأحكام القانونية الوطنية المنوط بها تنفيذ القرار. ويتناول التقييم أيضا نقطة جديدة تتمثل في أن استعراض تنفيذ أي صك يعتبر عملية تقنية أو صعبة، وتتطلب

تنفيذ قرار الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات

يكشف أحد التقارير المعنية بتنفيذ القرار الإطاري للاتحاد الأوروبي بشأن الهجمات ضد أنظمة المعلومات (2005) تباينا كبيرا في استعمال خيار عدم تجريم "الحالات البسيطة". واضطلعت الدول الأعضاء، على سبيل المثال، بما يلي:

- تجريم النفاذ إلى الحاسوب إذا ارتبط ذلك فقط بنية ارتكاب أعمال تجسس على البيانات.
- تجريم النفاذ غير المشروع في الحالات التي يتم فيها فقط إساءة استعمال البيانات أو إتلافها فيما بعد.
- تحديد تعرض البيانات للخطر عند الوصول إليها كشرط لقيام المسؤولية الجنائية.

كما أوضح التقرير بشكل عام أن: *"تباين تفسير وتطبيق خيار عدم التجريم لأفعال معينة يشكل خطرا جسيما على الهدف المتوخى من تقارب قواعد الدول الأعضاء بشأن القانون الجنائي في مجال الهجمات ضد نظم المعلومات"*.

المصدر: European Commission. 2008. COM (2008) 448 final.

---

[1] Cassese, A., 2005. *International Law*. Oxford: Oxford University Press, p.220-221.

[2] Klip, A., 2006. European Integration and Harmonisation and Criminal Law. *In:* Curtin, D.M. et al. European integration and law: four contributions on the interplay between European integration and European and national law to celebrate the 25th anniversary of Maastricht University's Faculty of Law. For general discussion, see Legrand, P., 1997. The Impossibility of 'Legal Transplants, *Maastricht Journal of European and Comparative Law*, (4):111-124

[3] European Commission. 2008. *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*. COM (2008) 448 final, Brussels, 14 July 2008.

وتجدر الإشارة إلى أن تنفيذ التحليل قد تم إجراؤه 20 دولة فقط من أصل 27 دولة من الدول الأعضاء في الاتحاد الأوروبي، واستند فقط على التحليل الرسمي للمعلومات المقدمة من الدول الأعضاء.

[4] Calderoni, F., 2010. The European legal framework on cybercrime: striving for an effective implementation. *Crime, Law and Social Change*, 54(5):339-357.

وقت، وموارد، وتنفيذا كاملا لكل من الأحكام التشريعية وتطبيقها عمليا.[1] ولا يدخل في نطاق وتَعْلِيمات هذه الدراسة الاضطلاع بأي شكل من أشكال التقييم للصكوك الدولية والإقليمية المختلفة والمنوط بها مكافحة الجريمة السيبرانية والمشار إليها في هذا الفصل.

وبالرغم من ذلك، يُظهر بشكل منفرد تحليل الردود على الاستبيان الخاص بهذه الدراسة أن عضوية صكوك متعددة الأطراف ترتبط مع التصور بزيادة *كِفَايَة* القانون الجنائي الوطني والقانون الإجرائي. كما يوضح أيضا الشكل 3-9 أن الدول المجيبة على الاستبيان الخاص بهذه الدراسة والتي لم تكن طرفا في إحدى الصكوك متعددة الأطراف المعنية بمكافحة الجريمة السيبرانية أفادت بـ "عدم كفاية" التجريم الوطني للجريمة السيبرانية والقانون الإجرائي على نحو أكثر تواترا.[2]

تنفيذ المشروع التوجيهي للجماعة الاقتصادية لدول غرب أفريقيا

في عام 2008، اعتمدت إحدى دول غرب أفريقيا قانونا بشأن التحقق من امتثال نظام الحواسيب للقوانين والأنظمة والمبادئ التوجيهية المنصوص عليها على المستوى الإقليمي من جانب الجماعة الاقتصادية لدول غرب أفريقيا (إيكواس) بشأن الجريمة السيبرانية، بيد أن هذا القانون تضمن تعديلات محددة:

- تعيين جرائم محددة لتكنولوجيا المعلومات في مجالات الحماية الجنائية التي تشتمل على تكنولوجيا المعلومات والبيانات الإلكترونية، والمحتوى الحاسوبي غير الشرعي، واستعمال الحاسوب في الاحتيال، وخدمات المساعدة الفنية، والإعلان الرقمي؛
- تحديث التشريعات المتعلقة بالجرائم الموجودة بحيث تتوافق مع بيئة تكنولوجيا المعلومات/الاتصالات الجديدة (في مجالات الحماية الجنائية ضد السرقة، الأضرار المادية التي تلحق بالممتلكات، وما إلى ذلك)؛
- إجراء تعديلات على قانون الإجراءات الجنائية لتنفيذ الصكوك الخاصة المعنية بتكنولوجيا المعلومات؛
- إرساء مبادئ توجيهية جديدة بشأن التعاون المتعلق بالأمور السيبرانية فيما يتعلق بدول الإيكواس، ومجلس أوروبا، والتعاون بين الدولة وإيكواس/مجلس أوروبا/مجموعة الثماني.

المصدر: Mouhamadou, L.O. 2011 الجريمة السيبرانية والحريات المدنية والخصوصية في المجتمع الاقتصادي لغرب أفريقيا. المؤتمر السنوي الـ 21 بشأن الحواسيب والحرية والخصوصية 2011.

بيد أنه من الممكن إثبات العلاقة بين "كفاية" التشريع و"عضوية الصك"، إلا أن الردود على الاستبيان المرافق لهذه الدراسة لم تكشف عن نمط واضح بين "المواءمة المتصورة" و"عضوية الصك". وعلى النحو المذكور أعلاه؛ فإن إدراك دول في أوروبا، على سبيل المثال، لمستويات عالية من المواءمة مع "الصكوك متعددة الأطراف"، لا يعني دائما أنها أدركت مستويات عالية من المواءمة بين التشريعات الوطنية داخل الإقليم.[3]

---

[1] على سبيل المثال، تنطوي آلية استعراض تنفيذ اتفاقية الأمم المتحدة لمكافحة الفساد على مُفْرَدات تفصيلية تتعلق بعملية الاستعراض، علاوة على المبادئ التوجيهية للخبراء الحكوميين وموظفي الأمانة العامة في إجراء الاستعراضات القطرية. أنظر:
http://www.unodc.org/documents/treaties/UNCAC/Publications/ReviewMechanism BasicDocuments/Mechanism_for_the_Review_of_Implementation_-_Basic_Documents_-_E.pdf

[2] الاستبيان الخاص بدارسة الجريمة السيبرانية، السؤال رقم 19. ويعتبر الشكل 3-9 قد عدد الصكوك التالية التي تم التوقيع فيها أو التصديق عليها: اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، الاتفاقية العربية لمكافحة جرائم المعلومات، اتفاقية كومنولث الدول المستقلة، اتفاقية منظمة شنغهاي للتعاون.

[3] أنظر أعلاه، القسم 3-2 الاختلافات ومواءمة القوانين، مواءمة التشريعات.

وعلى نحو مماثل، لا تكشف الحسابات القائمة على المجموعتين المجيبتين المذكورتين أعلاه (الصك، ولا يوجد صك) عن الاختلافات في المستويات المدركة من المواءمة مع الدول الأخرى أو داخل الأقاليم بشكل خاص.[1] وعلى الرغم من ذلك؛ فإن طبيعة الصكوك متعددة الأطراف عادة ما تتجه نحو أداء دور في عملية المواءمة، كما أنه من الوارد أن تعكس أيضا تلك الردود الاختلافات في التصوّرات حول ما يجعل "المواءمة" في المقام الأول. وفي هذا الصدد، ذكرت عدد من الدول تجارب إيجابية لتنفيذ الصكوك متعددة الأطراف. وأخيرا، وفيما يتعلق بالإبلاغ عن نجاح عمليات المواءمة، فعلى سبيل المثال؛ ذكرت العديد من الدول المجيبة على الاستبيان الخاص بهذه الدراسة تجربة إيجابية تتعلق بإدراج أحكام من الصكوك مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية في القانون الوطني.[2]

الشكل 3–9: أثر الصكوك متعددة الأطراف على إدراك كفاية التشريعات



المصدر: إستبيان دراسة الجريمة السيبرانية. السؤال 19. (رقم=42)

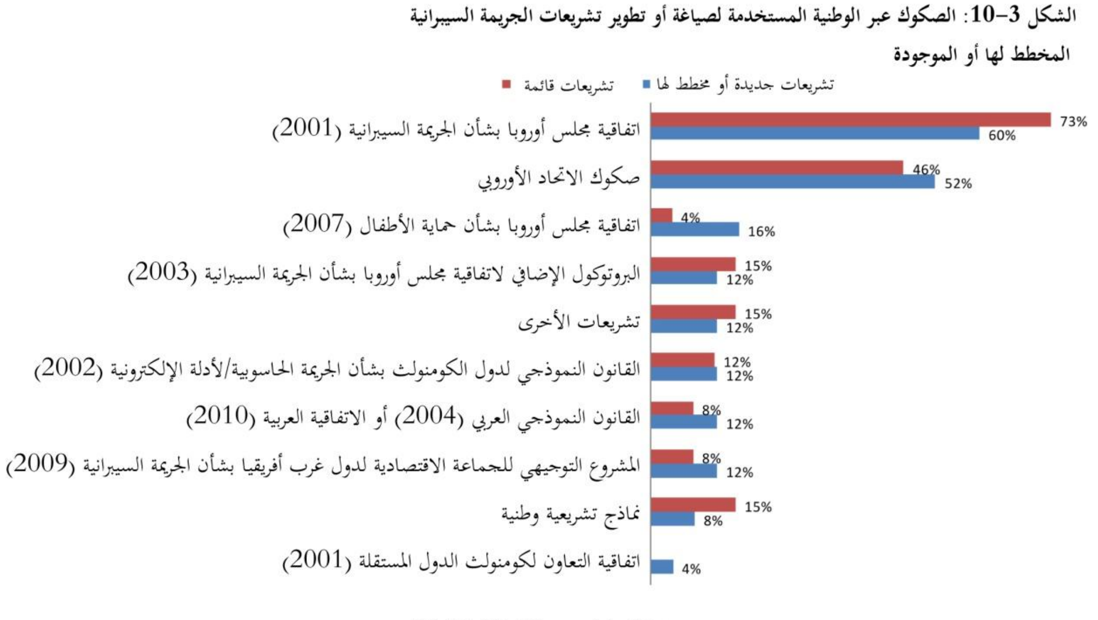
التأثير غير المباشر

بالإضافة إلى العضوية الرسمية في الصك وتنفيذه، فإن الصكوك متعددة الأطراف بشأن مكافحة الجريمة السيبرانية لديها تأثير غير مباشر على القوانين الوطنية، وهذا من خلال استعمال الدول الأطراف غير الأعضاء هذه الصكوك كنموذج، أو عن طريق تأثير تشريعات الدول الأطراف على تشريعات الدول الأخرى. هذا، ويجوز للدول استعمال أكثر من صك واحد لصياغة التشريع الوطني، حيث أفاد عدد من الدول بأن ذلك هو الحال بالنسبة لها.[3] وفي هذا الصدد، لُوحظ أن إحدى دول غرب أفريقيا، على سبيل المثال، تستخدم القانون النموذجي لدول اتحاد الكومنولث، والاتفاقية الأوروبية بشأن الجريم السيبرانية، والمشروع التوجيهي للجماعة الاقتصادية لدول غرب أفريقيا، وعلى هذا النمط، قامت دولة أخرى في غرب آسيا باستعمال كل من القانون النموذجي للدول العربية والأحكام التشريعية الوطنية لأحد الدول الأخرى في المنطقة.[4] وإلى جانب ذلك؛ وكما ذُكر آنفا، فإن الصكوك متعددة الأطراف ذاتها تتضمن قدرا كبيرا من الترابط بين النصوص. فعلى سبيل المثال؛ فقد تمت صياغة

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 17.
[2] الاستبيان الخاص بالدراسة، السؤال رقم 16.
[3] الاستبيان الخاص بالدراسة، السؤال رقم 12، والسؤال رقم 14
[4] المرجع السابق

القانون النموذجي لدول اتحاد الكومنولث وقرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات بإحكام عن كثب بما يتماشى مع اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.



المصدر: إستبيان دراسة الجريمة السيبرانية. السؤال 12 و14. (رقم=26، 25؛ 51، 50)

لقد عكست صعوبة التنفيذ المباشر للصكوك، والتأثير غير المباشر، ودمجهما النتائج الإجمالية المنبثقة عن الاستبيان الملحق بهذه الدراسة. ففي إطار جمع المعلومات الخاص بالدراسة؛ تم توجيه سؤال إلى الدول يتعلق باستخدامها الصكوك الدولية أو المحلية لصياغة أو تطوير التشريعات الحالية والجديدة أو المخطط لسنها.[1] وفي الواقع، قد أجاب عدد قليل نسبيا من الدول على هذا السؤال،[2] بيد أن الشكل 3-10، مع ذلك، يُظهر أن اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية والبروتوكول الإضافي الملحق بها استندت بشكل مباشر إلى اتفاقية مجلس أوروبا –مثل صكوك دول الاتحاد الأوروبي – والتي قد أُستخدمت على نطاق واسع لتطوير التشريعات المعنية بالجريمة السيبرانية. وإجمالا، استخدم حوالي نصف عدد هذه الدول صكوكا متعددة الأطراف مندرجة في "مجموعات"[3] دولية وإقليمية أخرى، مثل؛ الصكوك العربية والأفريقية، بالإضافة إلى استخدامها لتشريعات وطنية أخرى.

---

[1] المرجع السابق

[2] وتمثل التوزيع الإقليمي كالتالي: فيما يتعلق بالتشريعات القائمة؛ فيما يتعلق بالتشريعات القائمة: أوروبا 13؛ آسيا وأوقيانوسيا 7؛ الأمريكتين 5؛ أفريقيا 5؛ بشأن تشريع جديد أو المخطط له: أوروبا 7؛ آسيا وأوقيانوسيا 10؛ الأمريكتين 5؛ أفريقيا 6.

[3] أنظر أعلاه، القسم 3-3 نظرة عامة على الصكوك الدولية والإقليمية

وتجدر الإشارة هنا إلى أن هذا التقييم يعتبر قائما على ردود الدول وليس تناول محتوى القوانين الوطنية.[1] ويعتبر ذلك من المناسب إلى حد ما، حيث من المتَعَذّر بمجرد تحليل النصوص التشريعية، بشكل عام، تحديد أي من الصكوك قد أُستخدمت بالضبط لصياغة التشريعات. ويمكن تتبع أي تأثير متى بينت إحدى الأطر الدولية المحددة – والتي تظهر بعض الاختلافات التي يمكن تمييزها عن كافة الصكوك الأخرى – الأسلوب المتبع لتجريم جريمة معينة. فعلى سبيل المثال، تُلحق اتفاقية كومنولث الدول المستقلة[2] عناصر إضافية للنفاذ غير المشروع (تأثيرات على البيانات) وتجريم توزيع الفيروسات الحاسوبية بطريقة معينة، كما يمكن من ناحية أخرى الحصول على الأحكام التابعة لهذا النهج وذلك من خلال تحليل مضمون الأحكام القانونية في العديد من الدول في أوروبا الشرقية وغرب آسيا.[3]

يتم تحديد الإمكانيات الإجمالية لنجاح المواءمة ودمج القانون الدولي في التشريع الوطني، إلى حد كبير، من خلال مدى قدرة الدول على إدراج المعايير الدولية في النظم الوطنية. ومن أجل ذلك، فإن الأمر يحتاج إلى رؤية قانونية وبيئة سياسية واجتماعية تتوفر فيها درجة عالية من الدعم لإجراء الإصلاحات التشريعية اللازمة والالتزام بذلك. وهذا يحدث على الأرجح عندما يكون لدى الدول قدرة على الحفاظ على التقاليد القانونية، فِيمَا لاتزال تفي بالتزاماتها الدولية التي اختارت أن تضطلع بها.

أفادت إحدى الدول المستجيبة في غرب آسيا، على سبيل المثال، بضرورة مراعاة "المجتمع" فيما يتعلق بالعادات والتقاليد،[4] بينما شددت أيضا إحدى دول غرب أفريقيا إلى جانب دولة من دول الأمريكتين على استخدام "المشاورات مع الجهات الفاعلة" كممارسة جيدة لضمان الحفاظ على التقاليد القانونية الوطنية. وفي حالات أخرى؛ فإن الدول قد لا تستطيع أن تدرك بعد الحاجة إلى تعزيز قانون مكافحة الجريمة السيبرانية. وفي هذا الصدد، على سبيل المثال، أفادت إحدى دول الجنوب الأفريقي بأنه منذ "تطوير البنية التحتية لتكنولوجيا المعلومات إلا أنها مازالت ضعيفة، وعليه لا يشكل تشريع جرائم الإنترنت حاجة ملحة".[5]

وختاما، فإن استعمال كل من الصكوك الدولية والإقليمية الملزمة وغير الملزمة يمثل مع ذلك فرصة مُهِمّة لتحقيق تقدم إيجابي نحو مزيد من الاكتفاء ومواءمة القوانين الوطنية، علاوة على تعزيز التعاون الدولي على المدى البعيد لمجابهة أي من التحديات العالمية. ويتناول أيضا الفصل الرابع (التجريم) والفصل الخامس (التحقيقات وإنفاذ القانون) والفصل الثامن (المنع) كلا من التقارب والتباين في هذه المجالات الفردية.

---

[1] من الملاحظ أن بعض النتائج التي تم عرضها في الفصل الرابع (التجريم) والفصل الخامس (التحقيقات وإنفاذ القانون) في هذه الدراسة تستند إلى تحليل المصدر الرئيسي للتشريع.

[2] الفقرة (1/أ) من المادة الثالثة من اتفاقية كومنولث الدول المستقلة؛ "يتسبب النفاذ غير المشروع للمعلومات الحاسوبية المحمية بالقانون، في اتلاف البيانات أو إغلاقها أو تعديلها أو نسخها، أو تَعْطِيل وظائف الحاسوب أو نظم الحاسوب أو الشبكات ذات الصلة".

[3] أُنظر الفصل الرابع (التجريم)

[4] الاستبيان الخاص بالدراسة، السؤال رقم 16.

[5] المرجع السابق.

الفصل الرابع: التجريم

يقدم هذا الفصل تحليلا مُقَارَنا لأفعال الجريمة السيبرانية الواردة في القانون الدولي والقانون الوطني. كما يجسِّد نوعا من توافق الآراء الأساسية بشأن الحاجة إلى تجريم مجموعة من الأفعال التي تشكل الجريمة السيبرانية. ومع ذلك، يُظهر تناول أركان الجريمة عن قرب وجود تباين بين الدول والصكوك متعددة الأطراف المعنية بمكافحة الجريمة السيبرانية. أيضا، يبَيِّن هذا الفصل أثر الـ"سيف والدرع" للقانون الدولي لحقوق الإنسان على تجريم الجريمة السيبرانية.

1-4 استعراض عام للتجريم

الاستنتاجات الرئيسية

- وتبيَّن من إجابات البلدان على الاستبيان أنَّ هذه الأفعال الـ 14 مجرَّمة على نطاق واسع، باستثناء الجرائم المتعلقة برسائل البريد الإلكتروني الطفيلية بصفة رئيسية، وكذلك إلى حد ما الجرائم المتعلقة بأدوات إساءة استعمال الحواسيب والعنصرية وكراهية الأجانب وإغواء أو "مراودة" الأطفال على الإنترنت
- ويجسِّد هذا الأمر نوعا من توافق الآراء الأساسي على ما يُعاقب عليه من السلوكيات الإجرامية السيبرانية
- تعتبر الأفعال السيبرانية الأساسية التي تمس بسرية النظم الحاسوبية وسلامتها وقواعد النفاذ إليها مجرّمة في العديد من الدول باعتبارها من الجريمة السيبرانية الخاصة
- تعتبر الأفعال المرتكبة بواسطة الحواسيب والتي تشتمل على خرق السرية أو الاحتيال أو التزوير أو ارتكاب جرائم متصلة بالهوية مجرمة في أغلب الأحيان باعتبارها من الجرائم العامة
- تفيد نسبة 80 في المائة من الدول في أوروبا بكفاية تجريم الأفعال التي تشكل الجريمة السيبرانية
- أما في مناطق أخرى من العالم، تفيد نسبة تصل إلى 60 في المائة من الدول بعدم كفاية تجريم الأفعال التي تشكل الجريمة السيبرانية

يتمثل الهدف من هذه الدراسة في تقديم تحليل مقارن للجريمة السيبرانية المقننة في القانون الدولي والقانون الوطني، إلى جانب الاختلافات بين التشريعات الوطنية في مجال الجريمة السيبرانية، ومن ثم يُعتبر اسْتِيعاب نهج التجريم المستخدم من الأمور الهامة لثلاثة أسباب؛ أولها: أن الفجوات التي تعتري التجريم في أي دولة قد تُؤَمّن ملاذا للجاني، مع احتمالية أن تتأثر الدول الأخرى بذلك على الصعيد العالمي، وذلك على النحو الذي تم تناوله

في الفصل الثالث (التشريعات والأطر)، ثانيها: تمثل اختلافات التجريم مدخلا لتحديات التعاون الدولي الفعّال في المسائل الجنائية التي تنطوي على أفعال الجريمة السيبرانية، ولاسيما؛ فيما يتعلق بمبدأ ازدواجية التجريم، ثالثها: إن إجراء تحليل مقارن للجريمة السيبرانية يكشف النقاب عن الممارسات الجيدة التي يمكن أن تلجأ إليها الدول في سن القوانين الوطنية، طبقا للمعايير الدولية الناشئة في هذا المجال. ويلقي القسم التالي الضوء على تجريم الجريمة السيبرانية، حيث يتناول الفصل ماهية الطرائق المحددة التي تنتهجها الدول في تضمين عدد من الجرائم السيبرانية في القوانين الوطنية، ويختتم الفصل بمناقشة تتعلق بتأثير القانون الدولي لحقوق الإنسان على تجريم أفعال الجريمة السيبرانية.

الجريمة السيبرانية الخاصة، والجرائم العامة

من المفترض أن تتصدى الدول للأفعال الفردية التي تشكل الجريمة السيبرانية (مثل تلك التي تم تحديدها في الفصل الأول) من خلال عدد من الطرق، مع ملاحظة أن بعضا من هذه الأفعال لا يشكل مطلقا جريمة جنائية في القانون الوطني. ولئن اعتبرت هذه الأفعال من قبيل الأعمال الإجرامية، فقد تُدرج تحت الجرائم العامة (قانون الجرائم غير السيبرانية) أو الجريمة السيبرانية المحددة المتخصصة، أما فيما يتعلق بالأفعال الأخرى، فقد لا تعتبر عملا إجراميا، ولكنها تخضع إلى الجزاءات الإدارية أو الجزاءات المدنية. وفي هذا الصدد؛ أشار عدد من الدول المجيبة على الاستبيان الخاص بهذه الدراسة أن الجزاءات الإدارية تسري على مجموعة من الأفعال التي لا تعتبر من قبيل الأعمال الإجرامية، ومنها جرائم انتهاك حقوق التأليف والنشر وجرائم تقليد العلامات التجارية أو التحكم في إرسال رسائل إلكترونية مزعجة، بالإضافة إلى الأفعال التي تنطوي على انتهاك الخصوصية وإنتاج أو توزيع أو حيازة أدوات إساءة استخدام الحاسوب.[1] ويجب التنبيه؛ بأن هذا الفصل لا يتناول استخدام الجزاءات الإدارية أو الجزاءات المدنية، بل بالأحرى يركز على التجريم. ويبدأ الفصل بلمحة عامة عن ماهية نطاق تجريم الأفعال المختلفة للجريمة السيبرانية، وذلك قبل التعرض لمضمون الأحكام القانونية الوطنية.

ويقدم الشكل 4-1 نظرة عامة شاملة عن نطاق تجريم 14 فعلا من فئات الجريمة السيبرانية، كما ورد من 60 دولة من الدول المجيبة على الاستبيان الملحق بهذه الدراسة، حيث تدُلّ الردود على تجريم عدد 14 فعلا من أفعال الجريمة السيبرانية على نطاق واسع، باستثناء الجرائم المتعلقة بالرسائل الإلكترونية الاقتحامية بصفة رئيسية، وكذلك إلى حد ما الجرائم المتعلقة بأدوات إساءة استعمال الحواسيب والعنصرية وكراهية الأجانب وإغواء أو "مراودة" الأطفال على الإنترنت.[2] ويجسّد هذا الأمر نوعا من توافق الآراء الأساسي على ما يُعاقب عليه من السلوكيات الإجرامية السيبرانية. وكما لُوحظ في الفصل الأول (الموصلية والإنترنت)، فإن الدول قد أبلغت عن بعض الجرائم الإضافية غير المذكورة في الاستبيان، والمتعلقة بصفة رئيسية بمحتوى الحواسيب، بما في ذلك تجريم

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 25-39.

[2] المرجع السابق.

المواد الفاحشة ولعب القمار على الإنترنت والأسواق غير المشروعة على الإنترنت من قبيل أسواق الاتجار بالمخدرات والبشر. هذا، وقد تمت مناقشة الاستعانة بالقانون الجنائي لتنظيم محتوى الحاسوب والإنترنت على وجه الخصوص لاحقا في هذا الفصل، وذلك في سياق تأثير القانون الدولي لحقوق الإنسان على التجريم.

يُظهر أيضا الشكل (4-1) نموذجا واضحا لاستخدام القانون المعني بمكافحة الجرائم الخاصة بالفضاء السيبراني لتحديد الجريمة السيبرانية الأساسية التي تمس بسرية النظم الحاسوبية وسلامتها وقواعد النفاذ إليها، حيث تعتبر الجرائم الخاصة بالفضاء السيبراني ذات استعمال أقل عادة لأفعال الجريمة السيبرانية الأخرى، مثل استخدام الحاسوب في تحقيق مكاسب مالية أو شخصية أو تسبيب الضرر، أو استعمال الحاسوب في الأعمال ذات الصلة بالمحتوى. وعلى النقيض من ذلك؛ فإن دور الجرائم الإجرامية العامة يمثل أمرا هامّا لهاتين الفئتين الأخيرتين. وبشكل خاص، تفيد بعض الدول بأنها تضطلع باستعمال الجرائم العامة حتى للأفعال السيبرانية الأساسية، مثل النفاذ غير المشروع لجهاز الحاسوب أو البيانات الحاسوبية، أو اختراق البيانات الحاسوبية بصورة غير شرعية أو إلحاق ضرر بنظام الحاسوب. هذا، وقد تم تناول التوزيع بين الجرائم الخاصة بالفضاء السيبراني والجرائم العامة للأفعال المختارة بمزيد من التفصيل لاحقا في هذا الفصل.

الشكل 4–1: النهج الوطنية لتجريم أفعال الجريمة السيبرانية



المصدر: إستبيان دراسة الجريمة السيبرانية. السؤال 25–38. (رقم=61)

ويدعم التوزيع الواسع بين الجريمة السيبرانية الخاصة والجرائم العامة النهج المستنبط على الصعيد الدولي لوصف محل الجريمة السيبرانية ضمن نطاق الجريمة ككل. حيث إن مجلس الأمم المتحدة الاقتصادي والاجتماعي فرض الاضطلاع للقيام بعمل مبدئيّ بشأن "إطار دولي لتصنيف الجرائم"،[1] فعلى سبيل المثال؛ تصنف بعض من أفعال الجريمة السيبرانية على مستوى "رأسي" (كما في فئات الجريمة حيث يستبعد كل طرف منها الآخر) ولكن

---

[1] المجلس الاقتصادي والاجتماعي للأمم المتحدة، 2012. القرار 2012/18، بشأن تحسين نوعية الإحصاءات عن الجريمة والعدالة الجنائية مع توافرها.

أيضا تصور أفعال الجريمة السيبرانية المتوخاة على مستوى "أفقي"، باعتباره أحد "سمات" الجرائم التقليدية التي تنطوي على عنصر حاسوبي.[1]

إلى جانب تناول الطبيعة السيبرانية الخاصة أو العامة لأفعال الجريمة السيبرانية، فإن من المهم أيضا أخذ القانون الجنائي العام بعين الاعتبار، حيث إنه من المستقر عدم سريان أو تفسير الجريمة السيبرانية في القوانين الوطنية بمعزل عن نظام العدالة الجنائية، بل بالأحرى تطبق القواعد المعمول بها على كافة الجرائم، مثل؛ قواعد المساهمة الجنائية والشروع والإهمال والحالة الذهنية للجاني والدفوع القانونية. وفيما يتعلق "بالحالة الذهنية" بشكل خاص، فإنه يجب توخي الحذر عند اسْتِعْمال القانون المقارن، وعلة ذلك؛ أن النظم القانونية المختلفة تستعمل مجموعة كبيرة من المفاهيم والتعاريف المختلفة، علاوة على أن المصطلحات ذاتها في النظم القانونية المختلفة قد يكون لها معان مختلفة، إلى جانب ذلك أيضا، قد تميز النظم القانونية بين "الإرادة" و"الإدراك"، أو تحدد مجموعة من الحالات الذهنية التي تقود الجاني، مثل "القصد"، "مع الإدراك"، "متهور"، "إهمال".[2] ومع ذلك، ففي كل الأنظمة القانونية يندرج كل من سلوك الجاني "المتعمد" و"غير المتعمد" تحت طائلة المسؤولية.[3]

يعتبر هذا التمييز من قبيل الأمور الهامة عندما يتعلق الأمر بالجريمة السيبرانية، حيث يشير عدد من الصكوك الدولية والإقليمية، على سبيل المثال، إلى أن "*الجريمة تعتبر اقترفت عمدا*" متى شكل السلوك فعلا إجراميا.[1] أما فيما يتعلق بالصكوك الأخرى، فإنها تعتبر الرُعُونَة سببا من أسباب ارتكاب الجرائم الجنائية، حيث ينص مشروع اتفاقية الاتحاد الأفريقي، على سبيل المثال، على أنه ينبغي لكل دولة من الدول الأعضاء في الاتحاد الأفريقي أن تتخذ التدابير التشريعية اللازمة وأن تعتبر الإهمال لمعالجة البيانات الشخصية بدون اتباع القواعد الضرورية لمعالجة البيانات "جرما" في واقع الأمر،[2] كما أنه وفي بعض الدول الأفريقية، يعتبر أيضا السلوك الذي يصاحبه "تحايل" من العناصر الذهنية (الركن المعنوي) التي ترد عادة في قانون العقوبات. وفي هذا الصدد أيضا، يتضمن على سبيل المثال المشروع التوجيهي للجماعة الاقتصادية لدول غرب أفريقيا، بنودا مثل "الاعتراض الاحتيالي للبيانات الحاسوبية" و"النفاذ الاحتيالي لنظم الحاسوب".[3] وفي هذا السياق، قد يعتبر مستوى الهَدَف المطلوب موازيا لأحد أشكال الدلالات التحايلية، أي أكثر من المعيار العام "للفعل المتعمد"، ولكن أقل من غايَة خاصة تهدف إلى الحصول على الأموال أو السلع أو الخدمات، عن طريق الخداع أو الكذب.

وأخيرا، يتعين تحديد الركن المعنوي للأفعال التي تشكل الجريمة السيبرانية بشكل واضح في القانون، نظرا إلى أرجحية النطاق الواسع لبعض أفعال الجريمة السيبرانية، مثل النفاذ غير المشروع للبيانات الحاسوبية. وحيثما كان

---

[1] أُنظر: مركز التميز البحثي المعني بالمعلومات الإحصائية عن الحكومة، والجريمة والإيذاء والعدالة، 2012، تقرير الاجتماع التشاوري بشأن إطار دولي لتصنيف الجرائم. 17-19 تشرين الأول/أكتوبر 2012 مكسيكو سيتي.

[2] لفئات الركن المعنوي للجريمة في القانون القاري الأوروبي، أُنظر على سبيل المثال:
Roxin, C., 2010. *Strafrecht AT I*. 4th ed. Munich. pp.436 et seq. and 1062 et seq. (Germany); Picotti, L., 1993. *Il dolo specific*. Milan (Italy). For the categories of the mental element in common law countries, see Dressler, J., 2012. *Understanding Criminal Law*. 6th ed. pp.117–144 (United States); Ashworth, A., 2009. *Principles of Criminal Law*. 6th ed. pp.75, 154-156, 170-191 (United Kingdom).

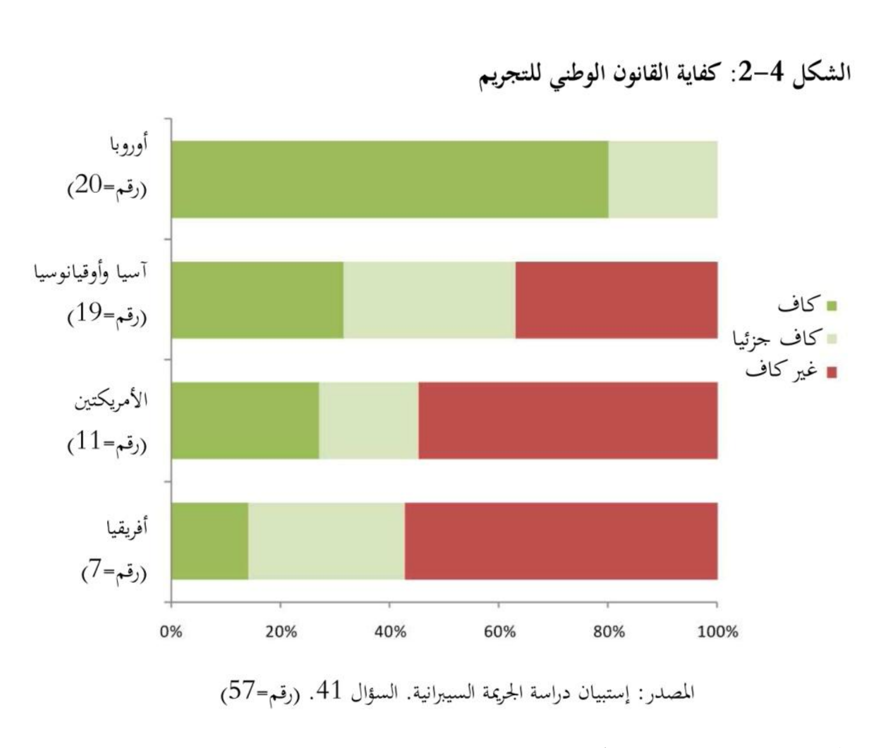
[3] "التعمد"، يشمل بشكل خاص الإرادة والعلم، أما مجموعة السلوك "غير العمدي" تتراوح بين التهور، الإهمال البسيط والإهمال الجسيم.

ذلك ممكنا، فإن التحليل التشريعي في هذا الفصل يسعى إلى تحديد أوجه التشابه والاختلاف في الأركان الدلالية للجريمة، حيث قد يكون ذلك في الجريمة ذاتها، أو من خلال القانون الجنائي العام.

كفاية القوانين الجنائية للجريمة السيبرانية

بالإضافة إلى تنوع النهج التشريعي الجنائي، تُظهر بعض الدول اختلافات في الكفاية المتصورة لأطرها المعنية بتجريم أفعال الجريمة السيبرانية. وقد أفاد ما يقرب من 80 في المائة من الدول الأوروبية، التي أجابت على الاستبيان الملحق بهذه الدراسة، بكفاية قوانينها الجنائية لمواجهة الجريمة السيبرانية، بيد أن باقي الدول أفادت بأن قوانينها كافية "بشكل جزئي". وعلى النقيض من ذلك، ففي مناطق أخرى من العالم؛ أفاد ما يقرب من 60 في المائة من الدول بعدم كفاية أطرها الجنائية لمواجهة الجريمة السيبرانية.

الشكل 4-2: كفاية القانون الوطني للتجريم



المصدر: إستبيان دراسة الجريمة السيبرانية. السؤال 41. (رقم=57)

وعندما وجه سؤال حول ماهية *الفجوات* الرئيسية في القانون الجنائي المعني بمكافحة الجريمة السيبرانية، أشارت العديد من الدول إلى حقيقية مفادها أن القوانين الجنائية-بصفة عامة-لا تتناسب بشكل واضح مَع الجريمة السيبرانية، أو نظرا لعدم وجود جرائم نَظِير سلوك سيبراني مُعَيّن. وفي هذا الشأن، أفادت إحدى الدول الأفريقية، على سبيل المثال، "*بعدم وجود جرائم ذات طبيعة سيبرانية أو تتعلق بالمعلومات*"، كما أشارت إحدى الدول الأخرى في غرب آسيا إلى أن المشكلة العامة تتمثل في "*أن طبيعة أشكال الجريمة والأركان الأساسية لها الواردة في القانون الجنائي تحول دون تطبيقه على الجرائم الإلكترونية*". وبشكل مماثل، ذكرت أيضا إحدى دول جنوب آسيا أن "*هناك حاجة إلى قانون [قوانين] مفصل ومحدد يعمل على تغطية جوانب مختلفة من الأفعال السيبرانية ذات الصلة باقتراف إحدى الجرائم. بيد أنه بكل*

---

[1] أنظر على سبيل المثال: اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المواد 2-9

[2] مشروع اتفاقية الاتحاد الأفريقي، القسم الرابع، القسم 3، المادة 29/ج

[3] المشروع التوجيهي للجماعة الاقتصادية لدول غرب أفريقيا، المواد 2-11

أسف لا زلنا في انتظار أحد تلك القوانين التي لم يتم الموافقة عليها بعد." [1] وفيما يتعلق بالفجوات التي تعتري السوك المحدد؛ أفادت إحدى الدول في غرب آسيا بأنه *"توجد فجوة قانونية تتعلق بتجريم سرقة البيانات لتحقيق مكاسب مالية*". أيضا ذكرت إحدى الدول في منطقة الكاريبي أنه *"لا توجد قوانين محددة تتعامل مع إرسال البريد الإلكتروني الطفيلي، واستعمال الحاسوب في أفعال تنطوي على العنصرية وكراهية الأجانب والتميز والإرهاب السيبراني وسرقة الهوية، وغيرها من الجرائم ذات الصلة*"، وعلى نفس المنوال، أفادت إحدى دول جنوب شرق آسيا أن "*بعضا من الجرائم السيبرانية المحددة لا تعتبر في الوقت الحالي بمثابة جريمة جنائية، مثل هجمات حجب الخدمة والبريد الإلكتروني الطفيلي*". كما أفادت العديد من الدول بوجود حاجة لتشريع يتعامل إلى حد كبير مع السلوك السيبراني المحدد. فعلى سبيل المثال، ذكرت إحدى الدول الأوروبية أنه "لا *يتم في الوقت الحالي تجريم شبكات الروبوت، وانتحال الشخصية واستمالة الطفل*"، إلى جانب ذلك، أشارت دولة أخرى من دول جنوب شرق آسيا، إلى إنه "*لم يتم في الوقت الحالي التصدي بشكل كاف للتحرش عبر الإنترنت، والتعقب السيبراني، وبعض الجرائم ذات الصلة بالهوية*". [2]

على العَكْس مما ذكر، فقد أفادت الدول أيضا بأن هناك العديد من نقاط القوة والممارسات الجيدة في تجريم الأفعال التي تشكل الجريمة السيبرانية. فعلى سبيل المثال؛ أشارت إحدى دول أمريكا الشمالية إلى أنه يعتبر من قبيل الممارسات الجيدة، أن يكون لدى الدولة *"تغطية واسعة لأفعال الجريمة السيبرانية بشكل محايد تكنولوجيا"* . كما أفات أيضا إحدى دول جنوب شرق آسيا بأن اتباع منهج مختلط للجرائم السيبرانية الخاصة والجرائم العامة كان يتسم بالفعالية، مثل "*جرائم السرية الحاسوبية التي يتناولها بشكل كامل قانون إساءة استعمال الحاسوب، [و] قد تصدت إلى حد كبير قوانين لا تتعلق بالجريمة السيبرانية لمعظم الأشكال الأخرى من الجريمة السيبرانية*". وأخيرا، فقد سلطت إحدى الدول في أوقيانوسيا الضوء على الحاجة إلى "تغطية *واسعة لأفعال الجريمة السيبرانية*"، إلى جانب أهمية وجود ردع من خلال *"العقوبات الصارمة*". [3]

[1] الاستبيان الخاص بالدارسة، السؤال رقم 41

[2] المرجع السابق

[3] المرجع السابق

2-4 تحليل الجرائم الخاصة

الاستنتاجات الرئيسية:

- بينما يوجد توافق عامّ بشأن مجالات التجريم الواسعة، فإن التحليل المفصل للأحكام الواردة في مصدر التشريع تكشف النقاب عن تباين النُهُج بشكل واضح على المستوى الوطني، وفي بعض الحالات، على المستوى الدولي
- تفاصيل المسائل المتعلقة بالجريمة السيبرانية. يمكن أن تُجسد الاختلافات في أركان الجرائم تحديات عند مُسَاواتها بالجرائم المقننة في دول مختلفة، وذلك لأغراض التعاون الدولي. وقد يؤدي تغير بسيط في أركان الجريمة، مثل تَمْدِيد "الأفعال غير المتعمدة" في الركن المعنوي للجريمة، إلى خطر المغالاة في عملية التجريم
- تتباين الجرائم التي تنطوي على نفاذ غير مشروع لنظم الحاسوب أو البيانات الحاسوبية من حيث محل الجريمة (بيانات، نظام، أو معلومات)، ومستوى التجريم، أي تجريم النفاذ بحد ذاته "فحسب" أو شرط التحايل على التدابير الأمنية أو اقتضاء وجود نية أخرى كامنة في النفاذ، ومن ذلك مثلا التسبُّب بخسائر أو أضرار
- ويختلف تجريم التدخُّل غير المشروع تبعا لما إذا كان الجُرم محصورا بنقل البيانات غير العمومية، أو ما إذا كان الجُرم محصورا بالتدخُّل "بواسطة الوسائل التقنية"
- تقتضي معظم البلدان أن يكون التدخُّل في النظم أو البيانات متعمَّدا لكي يعتبَر جريمة، في حين تجرِّم بلدان أخرى التدخُّل دونما اكتراث فيها
- ولا تجرِّم جميع البلدان أدوات إساءة استعمال الحواسيب. أما في البلدان التي تجرِّمها، فتبرز الاختلافات تبعا لما إذا كان الجُرم يشمل استعمال برمجيات و/أو رموز النفاذ إلى الحواسيب. توجد أيضا اختلافات ما إذا كان القانون يشترط أن تكون الأداة نفسها قد صممت خصيصا لارتكاب أحد الجرائم، و/أو اتجهت نية الجاني إلى استعمالها لارتكاب أحد الجرائم
- تستخدم القوانين الوطنية بشأن استغلال الطفل في المواد الإباحية مجموعة من المصطلحات ولكن فقط حوالي ثلث الدول تستعمل المواد المصمَّمة بالمحاكاة، والأفعال المشمولة بها. وتحدد غالبية البلدان الفئة العمرية لاستغلال الطفل في المواد الإباحية بسن 18 عاما، ولكن بعض الدول تستخدم حدودا عمرية أصغر. ويجرم حوالي ثلثي الدول حيازة الصور الإباحية للأطفال

يتناول هذا القسم من الفصل تحليلا مفصلا للأحكام المتعلقة بالجريمة السيبرانية الواردة في القوانين الوطنية بغية تحديد كل من الاختلافات بين الدول التي قد تولد تحديا لمواءمة تشريعات الجريمة السيبرانية، والعناصر المشتركة للجرائم التي يمكن اعتبارها من قبيل الممارسات الجيدة. ويستند هذا التحليل إلى مصدرين، أولهما: ردود الدول على الاستبيان الخاص بهذه الدراسة، وثانيهما: تحليل المصدر الرئيسي للتشريع لمجموعة عريضة من الدول تصل إلى 100 دولة تقريبا.[1] وخلال هذا القسم، ستتم الإشارة إلى المصدر المستخدم في كل مرحلة.[2] وبشكل عام، تُستعمل ردود الدول على الاستبيان الملحق بهذه الدراسة في تقييم وجود إحدى الجرائم التي تشكل أحد الأفعال المعَيّنة للجريمة السيبرانية. أما بخصوص الدول التي تجرم فعل الجريمة السيبرانية، فإن تحليل المصدر الرئيسي للتشريع سيستخدم بعد ذلك في تناول محتويات الجريمة في القانون الوطني، وذلك باستخدام منهجية وظيفية قائمة على القانون المقارن.[3] وفيما يتعلق بتحليل المصدر الرئيسي للتشريع؛ فمن الملاحظ أن التشريع المعني بكل فعل معين من أفعال الجريمة السيبرانية غير متوفر من جميع الدول. وبالتالي؛ اضطلع عدد من الدول بتضمين هذا الجزء المعني بتفاوت التحليل طبقا للعمل الإجرامي للجريمة السيبرانية التي تم تناوله.[4]

الدخول/النفاذ إلى نظام حاسوبي بصورة غير مشروعة

يعتبر فعل اقتحام نظام حاسوبي بدون إذن شَرْعِيّ من الأفعال الموجودة مسبقا منذ الأيام الأولى لتطوير تكنولوجيا المعلومات،[5] حيث يشكل النفاذ غير المشروع تهديدات للمصالح مثل سلامة النظم الحاسوبية. فالاعتداء على المصالح القانونية ليس فقط عندما يقوم أحد الأشخاص، وبدون إذن مسبق، بتغيير أو "سرقة" البيانات الموجودة في نظام حاسوبي يخص شخصا آخر. بل أيضا عندما يقوم

نفاذ غير مشروع: اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

المادة 2 – النفاذ غير المشروع

يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغير تشريعية لكي يدرج في عداد الأعمال الإجرامية الاختراق المتعمد الكامل أو الجزئي لأحد أنظمة الحاسوب بدون وجه حق، وذلك بموجب قانونه الداخلي. ويجوز لأي طرف أن يشترط توافر نية الحصول على معلومات حاسوبية، أو أيا من النوايا الأخرى غير الشريفة، عند ارتكاب جريمة من خلال انتهاك التدابير الأمنية، أو عندما يتعلق الأمر بنظام حاسوبي متصل بنظام حاسوبي آخر.

---

[1] لقد تم تحليل المصدر الرئيسي للتشريع لـ 97 دولة، بما فيها 56 من الدول المجيبة على الاستبيان المرافق لهذه الدراسة. وكان التوزيع الإقليمي كالتالي: أفريقيا (15)، الأمريكتين (22)، وآسيا (24)، وأوروبا (30)، وأوقيانوسيا (6). بيد أنه كان من الجائز ضم 13 دولة من الدول المجيبة على الاستبيان المرافق لهذه الدراسة في التحليل الخاص بالمصدر الرئيسي للتشريع نظرا لعدم كفاية المعلومات بشأن التشريعات ذات الصلة الواردة في الاستبيان.

[2] سمات المصدر: (أ) الاستبيان المرافق لدراسة الجريمة السيبرانية، (ب) تحليل مكتب الأمم المتحدة المعني بالمخدرات والجريمة للتشريعات. ويجب ملاحظة أن تحليل المصدر الرئيسي للتشريع يعتبر غير قادر بسهولة على مراعاة التفاعلات القانونية بين الأحكام الخاصة والأجزاء العامة الأخرى للقانون الجنائي، أو تأثير القرار القضائي أو القانون التفسيري الأخر الذي يؤثر على قراءة الأحكام التشريعية الأصلية.

[3] للمزيد من المناهج المستخدمة في القانون الجنائي المقارن، أنظر:
Sieber, U., 2006. Strafrechtsvergleichung im Wandel. *In:* Sieber, U., Albrecht, H.J. *Strafrechtsvergleichung und Kriminologie unter einem Dach*. Berlin: Duncker & Humblot, pp.78 and 111-130.

[4] لقد تم تحليل عدد 90 دولة بحد أقصى (أحكام غير النفاذ المشروع)، وعدد 70 دولة كحد أدنى (الأحكام المعنية باستغلال الأطفال في المواد الإباحية وسوء استخدام أدوات الحاسوب).

[5] See Kabay, M., 2009. History of Computer Crime. *In:* Bosworth, S., Kabay, M.E. and Whyne, E., *Computer Security Handbook*. 5th ed. New York: Wiley; Sieber, U., 1986. *The International Handbook of Computer Crime*. Chichester: John Wiley & Sons, pp.86-90.

أحد الجناة "باستراق النّظَرَ" في النظام الحاسوبي، حيث يعتبر ذلك انتهاكا لسرية البيانات، وفي هذه الحالة قد يطُلب من المجني عليه إجراءات أَسَاسِيّة للتحقق من سلامة النظام الحاسوبي أو حالته. هذا، ولا يتطلب "مجرد" اقتحام نظام حاسوبي أو الاختراق "البَحْت" لنظام حاسوبي أن يصل الجاني لملفات النظام أو بيانات أخرى مخزنة. ومن ثم، فإن تجريم النفاذ غير المشروع للنظام الحاسوبي يعتبر ردعا هامّا للعديد من الأفعال اللاحقة الأخرى ضد السرية، والنزاهة، وتوافر البيانات ونظم الحاسوب، أو كذلك استعمال الحاسوب في ارتكاب جرائم أخرى مثل سرقة الهوية والأعمال ذات الصلة بالاحتيال والتزوير.[1]

وكنتيجة لذلك، يستلزم اعتماد الأحكام الواردة في الإحدى عشر صكّا المنوط بها تجريم اقتحام نظام أو بيانات حاسوبية بصورة غير شرعية،[2] حيث تعكس التشريعات هذا المطلب بشكل واضح على المستوى الوطني. يبَيّن الشكل 4-3 أن ما يقرب من 70 في المائة من الدول المجيبة على الاستبيان المرافق لهذه الدراسة قد أفادت بوجود جريمة سيبرانية خاصة تتمثل في النفاذ غير المشروع لأحد أنظمة الحاسوب.[3] إلى جانب ذلك، ذكر ما يقرب من 20 في المائة من الدول المجيبة أن الأحكام العامة للقانون الجنائي قد تناولت هذا الفعل. هذا، ويوجد عدد قليل جدا من الدول بنسبة تصل إلى 7 في المائة لم تجرم على الإطلاق، النفاذ غير المشروع لأحد أنظمة الحاسوب.

الشكل 4-3: تجريم الدخول غير المشروع إلى نظام حاسوبي

المصدر: إستبيان دراسة الجريمة السيبرانية. السؤال 25. (رقم=59)

يظهر تحليل المصدر الرئيسي للتشريع للأحكام المعنية بالنفاذ غير المشروع لنحو 90 دولة، خلافات عبر الحدود الوطنية فيما يتعلق بمحل الجريمة والأفعال التي تتناولها، بالإضافة إلى الركن المعنوي للجريمة.

محل الجريمة – تنص كافة الصكوك الدولية والإقليمية المعنية بالجريمة السيبرانية على تجريم النفاذ غير المشروع لنظام الحاسوب سواء كان كليا أو جزئيا. ومع ذلك، يتبع هذا النهج ما يقرب من نسبة 55 في المائة فقط من الدول المدرجة في تحليل المصدر الرئيسي للتشريع.

---

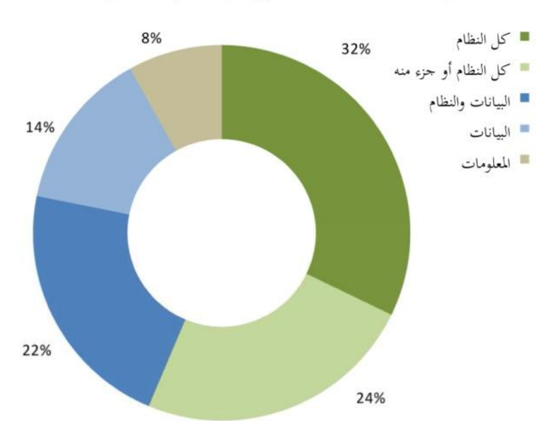
[1] See Council of Europe, 2001. *Explanatory Report to Council of Europe Cybercrime Convention*, ETS No. 185, para. 44: *'Illegal access covers the basic offense of dangerous threats to and attacks against the security (i.e., the confidentiality, integrity and availability) of computer systems and data.'*

[2] مشروع اتفاقية الاتحاد الأفريقي، المواد 15/ج، 16/ج، مشروع ميثاق الكوميسا المادتان 18و 19، القانون النموذجي لدول اتحاد الكومنولث المادة5، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المادة2، المشروع التوجيهي للجماعة الاقتصادية لدول غرب إفريقيا المادة 2، قرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات المادة1/2 مقترح توجيهي لدول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات المادة 3، النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات السلكة واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات المادة 4، الاتفاقية العربية بشأن مكافحة جرائم المعلومات المادة 6، القانون النموذجي للدول العربية المواد 3، 5، 15، و22، اتفاقية كومنولث الدو المستقلة المادة 3 (1/أ).

[3] الاستبيان الخاص بهذه الدراسة، السؤال رقم 25.

يبين الشكل 4-4 أن بعضا من القوانين الوطنية تعتبر البيانات أو المعلومات بمثابة محل جريمة النفاذ غير المشروع بدلا من النظام، أو أحيانا تجرم في أحكام مختلفة مسألة اقتحام نظام حاسوبي أو الاطلاع على بيانات حاسوبية بصورة غير شرعية. بيد أن بعض الدول تذهب إلى أبعد من ذلك في تَقْييد النهج المستخدم حيال ذلك.

الشكل 4-4: محل الدخول غير المشروع إلى نظام حاسوبي



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=87)

وفي هذا الصدد، وعلى سبيل المثال؛ تجرم عدة دول في غرب آسيا وشرق أوروبا الاختراق غير الشرعي "للمعلومات المحمية بموجب القانون".

الأفعال المشمولة – يشكل تجريم "مجرد" النفاذ غير المشروع، أو الشرط القاضي بتوافر مزيد من الأفعال أو النية نقطة خلافية أخرى، حيث تنص كافة الصكوك الدولية على خيار تجريم مجرد النفاذ غير المصرح به لنظام حاسوبي. ومع ذلك، تجيز بعض الصكوك مزيدا من الشروط. فعلى سبيل المثال؛ تمنح اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية،[1] والنصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات،[2] الدول إمكانية إرفاق شروط إضافية، مثل "التجاوز الأمني" أو "هدف احتيالي". ومن الملاحظ أن قرار الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات يمنح الدول الأعضاء فرصة لتجنب تجريم الحالات البسيطة.[3] هذا، وتشترط اتفاقية كومنولث الدول المستقلة لتجريم النفاذ غير الشرعي أن ينتج عنه "تعطيل أداء الحاسوب، أوتدميره أو إيقافه أو تعديله أو نسخ المعلومات المخزنة، ويسري ذلك أيضا على الشبكات ذات الصلة".[4]

دخول غير مشروع: مثال وطني من دولة في جنوب أوروبا

أي شخص يصل إلى نظام حاسوبي بدون تصريح قانوني أو تفويض من المالك أو صاحب الحق على النظام كله أو جزء منه، يعاقب بالحبس لمدة تصل إلى ـــــ سنة، أو بغرامة تصل إلى ـــــ.

غني عن البيان، أن هذه الشروط تمكن الدول من اعتماد تشريعات أضْيَق بشأن اقتحام نظام حاسوبي بصورة غير شرعية. في الواقع، لا يعتبر توافق الآراء بشأن الرغبة في تجريم مجرد النفاذ غير المشروع للأنظمة غير المحمية[5] ذا منحى عالَميّ. قد تقود بعض الشروط التي تنص عليها

[1] المادة الثانية من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

[2] المادة الخامسة من النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات /الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات

[3] المادة الثانية من قرار الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات

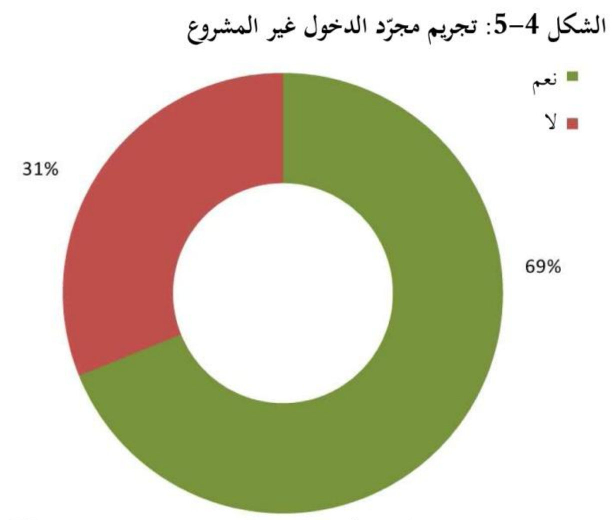
[4] الفقرة1/أ من المادة 3 من اتفاقية كومنولث الدول المستقلة.

[5] أنظر على سبيل المثال:
Sieber, U., 1985. *Informationstechnologie und Strafrechtsreform*. Cologne: Carl Heymanns Verlag, p.49.

النُهُج الدولية ولاسيما التي تشتمل على متطلبات إضافية بشأن الفعل الإجرامي، إلى تحديات تتمثل في تمييز النفاذ غير المشروع من الجرائم اللاحقة، مع احتمال تشابك الحدود بين النفاذ غير المشروع والجرائم الأخرى، مثل اعتراض البيانات أو التجسس على البيانات.

يوضح الشكل 4-5 أن نحو 70 في المائة، من بين تلك الدول التي تجرم الدخول غير المشروع، تُجرم مجرد الدخول غير المشروع لنظام حاسوبي، في حين أن النسبة الباقية، 30 في المائة، تضع شروطا إضافية للفعل الذي يشكل إحدى الجرائم السيبرانية، بيد أنه لا يوجد نمط إقليمي واضح لهذه النتيجة. فمن الملاحظ أن عددا قليلا من الدول تشترط إما "*انتهاك التدابير الأمنية*" أو هدفا إضافيا، مثل "*اتجاه نية الجاني إلى ارتكاب جريمة أخرى بجانب الجريمة الأصلية*"، كما أن بعض القوانين الوطنية تحصر النفاذ غير المشروع فقط في حالات "*الانتهاكات الجسيمة" أو الجرائم الخطيرة*"، كما هو الحال في إحدى بلدان أوقيانوسيا.[1] بالإضافة إلى ذلك، تجرم بعض القوانين الوطنية النفاذ غير المشروع فقط إذا تم "*نسخ" البيانات أو "حظرها"، أو "سرقتها"، أو "تعديلها"، أو حذفها*"، أو إذا ارتكب النفاذ غير المشروع *بالارتباط مع التدخل غير المشروع في النظام*". وفي بعض الدول، يجرم اقتحام نظام حاسوبي بصورة غير مشروعة باعتباره أحد جرائم التدخل غير المشروع في البيانات أو النظم. على سبيل المثال: تُجرِّم إحدى دول أوروبا الشرقية فعل "التدخل غير المشروع في البيانات أو النظم" فقط إذا ارتكب "بالتزامن" مع النفاذ غير المصرح به لأحد أنظمة الحاسوب، إلا أن ذلك له تأثير في الحد من تجريم التدخل غير المشروع في البيانات إلى الحالات التي يعتبر النفاذ غير المشروع خطوة أولى في ارتكاب الجريمة ضد البيانات والأنظمة.

الشكل 4-5: تجريم مجرّد الدخول غير المشروع



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=90)

الركن المعنوي – تشترط كل الصكوك متعددة الأطراف أن ترتكب جريمة اقتحام نظام حاسوبي بصورة غير مشروعة بشكل متعمد أو، في حالة وجود صكين، احتيالي.[2] ومع ذلك، جرت العادة أن يُترك تعريف ما يشكل اتجاه "نية الجاني" إلى الدولة المنفذة. فعلى سبيل المثال: ينص التقرير التَفْسِيرِيّ المرافق لاتفاقية مجلس أوروبا

---

[1] هذه الدولة تحصر التجريم للأفعال المرتكبة بقصد ارتكاب أو تسهيل ارتكاب جريمة خطيرة ضد أحد القوانين عن طريق النفاذ غير المشروع. وتُعرف الجريمة الخطيرة بأنها جريمة معاقب عليها بالسجن مدى الحياة أو على الأقل لمدة أكثر من خمس سنوات.

[2] مشروع اتفاقية الاتحاد الأفريقي المواد 15/ج، 16/ج؛ المشروع التوجيهي للجماعة الاقتصادية لدول غرب إفريقيا المادتان 2، و3.

بشأن الجريمة السيبرانية، صراحة على أنه يتعين تعريف المعني الدقيق "للفعل المتعمد" وفقا "للتفسير الوطني".[1] وفي هذا الشأن؛ وعلى النحو المذكور أعلاه، يختلف تشكيل الحالة الذهنية الصَحِيحة "للفعل المتعمد" بين العديد من الأنظمة القانونية الوطنية، تبعا للقانون الجنائي بقسميه العام والخاص.[2]

ومع ذلك؛ يظهر تحليل المصدر الرئيسي للتشريع – لتلك الأحكام المعنية بالنفاذ غير المشروع التي تدل بشكل خاص على الحالة الذهنية للجاني – أن الركن المعنوي المتمثل في "الفعل المتعمد"، و"العلم والإدراك"، و"الإصرار"، و"النية الاحتيالية" يشير إلى أن بعضا من أشكال الفعل المتعمد تشكل أغلب العناصر المطلوبة لقيام الجريمة. كما أنه من الملاحظ أنه من الجائز ارتكاب جريمة اقتحام نظام حاسوبي بصورة غير مشروعة "بشكل متهوّر"، وهذا ما عبر عنه تحليل المصدر الرئيسي للتشريع في دولتين من دول منطقة الكاريبي وأوقيانوسيا.

الظروف المشدِدَة – تتضمن أربعة صكوك دولية متعددة الأطراف بشأن مكافحة الجريمة السيبرانية ظروفا مُشَدِّدَة للعقوبة في الأحكام الخاصة باقتحام نظام حاسوبي بصورة غير مشروعة. [أولا]: ينص القانون العربي النموذجي لمكافحة الجريمة السيبرانية على تشديد العقوبات متى اقترن ارتكاب جريمة النفاذ غير المشروع *"بنية إلغاء أو حذف أو إتلاف أو تدمير أو الكشف عن أو تغير أو إعادة نشر البيانات أو المعلومات الشخصية"* (المادة 3)، كما تقتضي المادة (5) بتشديد العقوبة إذا ارتكب الجاني جريمة اقتحام نظام حاسوبي بصورة غير مشروعة *"عند اضطلاعه بمهامه، أو قام بتسهيل ارتكاب الجرائم من قبل طرف ثالث"*. [ثانيا]: تنص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على الظروف المشَدَّدَة للعقوبة إذا كان النفاذ إلى النظام الحاسوبي يؤدي إلى *"محْو البيانات المحفوظة أو تعديلها أو تحْريفها أو استنساخها أو إزالتها أو تدميرها، أو تدمير الأدَوات الإلكترونية وشبكات الاتصال والأنظمة الحاسوبية، وإلحاق أضرار بالمستخدمين أو المستفيدين، أو الحصول على معلومات حكومية سرية"* (المادة 6). [ثالثا]: قد أضاف مشروع الميثاق النموذجي للسوق المشتركة لشرق وجنوب أفريقيا أحكاما تتعلق بتجريم اقتحام *"نظام حاسوبي حكومي"* بصورة غير مشروعة أو استخدام أنظمة الحاسوب في عمليات البنية التحتية الحيوية" (المادة 19). [رابعا]: تطرح المادة (10) من المشروع التوجيهي لقرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات شروط تشديد العقوبات لارتكاب جرائم اقتحام نظام حاسوبي بصورة غير مشروعة: (1) أن يتم ذلك في إطار *"منظمة إجرامية"*، (2) أو من خلال استخدام *"إحدى الأدوات المصممة لشن هجمات تؤثر على عدد كبير من نظم المعلومات"* أو هجمات تتسبب في أضرار كبيرة، مثل

---

[1] مجلس أوروبا 2001، التقرير التَفْسِيريّ المرافق لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، سلسلة المعاهدات الأوروبية رقم 185، الفقرة 39: "يجب أن ترتكب كل الجرائم الواردة في الاتفاقية عمدا حتى تسري المسؤولية الجنائية. وفي حالات محددة؛ يشكل عنصر توافر النية الخاصة جزء من الجريمة. فعلى سبيل المثال، في المادة 8 المعنية باستخدام الحاسوب في ارتكاب أعمال الاحتيال؛ يعتبر توجه النية نحو تحقيق منفعة مادية بمثابة العنصر المكون للجريمة. وقد وافق واضعو الاتفاقية على أن المعني الدقيق لـ "الفعل العمدي" يجب أن يترك تعريفه إلى التفسير الوطني".

[2] أنظر على سبيل المثال:
LaFave, R.W., 2000. *Criminal Law*. 3rd ed. St. Paul: MN. pp. 224-234; Fletcher, G., 1998. *Basic Concepts of Criminal Law*. Oxford University Press, pp.99-100, 111-129; Fletcher, G., 1971. The Theory of Criminal Negligence: A Comparative Analysis. *University of Pennsylvania Law Review*, 119(3):401-403.

تعطيل خدمات النظام، تكبد نفقات مالية أو فقد البيانات الشخصية، (3) أو من خلال *"إخفاء الجاني الهوية الحقيقية"* والتسبب في إلحاق الضَرَر بالمالك القانوني للهوية.

أما على المستوى الوطني، فإن العديد من الدول التي تجرم مجرد النفاذ غير المشروع، تضطلع بدورها لتقنن ظروفا مشددة للعقوبة، بيد أن هذه الظروف تختلف من دولة إلى أخرى، وقد تم تحديدها كالتالي:

- ارتكاب الفعل بقصد مالي أو بقصد إلحاق ضرر؛
- التدخل غير المشروع في أداء أحد أنظمة الحاسوب؛
- طمس البيانات أو تغييرها؛
- نسخ برامج أو بيانات حاسوبية أو استعمالهما أو الإفصاح عن أي منها، أو أي انتهاك آخر من انتهاكات برامج الحاسوب والبيانات الحاسوبية؛
- اختراق جهاز حاسوب ثالث؛
- التسبب في إلحاق ضرر كبير؛
- إحداث فوضى عامة؛
- تسهيل أو دعم الإرهابي؛
- ارتكاب الفعل كعضو في جماعة منظمة؛
- اقتران الفعل بسلوك عنيف.

وكما ذكر أعلاه، فإن العديد من هذه الصكوك يظهر إمكانية وجود تداخل مع جرائم أخرى أو منفصلة، مثل التدخل غير المشروع في البيانات أو إتلاف النظام الحاسوبي. هذا، وقد أُكتشف خلال استعراض المصدر الرئيسي للتشريع أن أكثر الظروف المشددة للعقوبة بشكل سائد تمثلت، مع ذلك، في استخدام أنظمة الحاسوب في عمليات البنية التحتية الحيوية، مثل البنوك والاتصالات والخدمات الصحية والخدمات العامة أو أجهزة الحاسوب الحكومية. ويتضح مما تقدم، أن أكثر من نصف القوانين الوطنية التي تم تناولها منحت حماية خاصة تجسدت في زيادة العقوبات عند النفاذ غير المشروع لحاسوب حكومي أو قد يكون مرتبط بالأعمال الحيوية للبنية التحتية.

البقاء غير المشروع في نظام حاسوبي

يتناول صكان من الصكوك متعددة الأطراف تجريم "البقاء" في نظام حاسوبي بدون الحق في ممارسة ذلك بعد انتهاء مدة صلاحية الترخيص الممنوحة له، وذلك بجانب تجريم النفاذ غير المشروع لنظام حاسوبي.[1] وتمنح النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات حرية عدم

[1] المادة 3 من المشروع التوجيهي للجماعة الاقتصادية لدول غرب افريقيا، والمادة 5 النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات

تجريم مجرد البقاء في النظام بدون تصريح، شريطة أن تتوافر إجراءات فعالة أخرى. ومن ناحية ثانية؛ يشترط المشروع التوجيهي للجماعة الاقتصادية لدول غرب أفريقيا توافر الهدف الاحتيالي في البقاء في نظام حاسوبي بصورة غير قانونية.

تنعكس هذه الاختلافات في التشريعات الوطنية، حيث تدرج بعض القوانين مفهوم البقاء غير القانوني في الأحكام الخاصة باقتحام نظام حاسوبي بصورة غير مشروعة، بينما تفرد بعض القوانين الأخرى أحكاما خاصة بالبقاء غير القانوني. ومع ذلك، وبشكل أكثر شيوعا، فإن البقاء غير القانوني لم يُجرَّم بشكل خاص على الإطلاق. الدول التي أدرجت ضمن الدول الخاضعة إلى تحليل المصدر الرئيسي للتشريع، وجد أن تسع دول فقط، موزعة على مناطق، تُجرم البقاء غير القانوني، بينما قامت ثماني دول بتجريم ذلك من خلال إدراجه في الأحكام الخاصة باقتحام نظام حاسوبي بصورة غير مشروعة، في حين قامت دولة واحدة بتجريم البقاء غير القانوني في حكم مستقل بذاته.

البقاء غير المشروع: المشروع التوجيهي للإيكواس

المادة 3 – البقاء في نظام حاسوبي بشكل احتيالي

هو الفعل الذي يقوم بموجبه شخص بالبقاء أو محاولة البقاء في كل النظام الحاسوبي أو جزء منه.

الاعتراض غير المشروع للبيانات الحاسوبية

يمتد تجريم الاعتراض غير القانوني بداية من حماية سلامة وسرية البيانات الحاسوبية والبيانات المستقرة في أحد الأنظمة الحاسوبية إلى البيانات المرسلة. ويتجسد أحد الشواغل الرئيسية وراء حظر اعتراض البيانات الحاسوبية عند إرسالها في انتهاك سرية المراسلات الخاصة.[1]

تتضمن تسعة صكوك دولية أحكاما خاصة بتجريم اعتراض البيانات الحاسوبية.[2] فعلى المستوى الوطني، من الملاحظ أن لدى العديد من الدول جرائم محددة تغطي اعتراض البيانات الحاسوبية، ومنها حظر اعتراض المراسلات بشكل عام، في حين أن الدول

الاعتراض غير المشروع: المشروع التوجيهي للإيكواس

المادة (6) – الاعتراض الاحتيالي للبيانات الحاسوبية

هو قيام شخص باعتراض أو محاولة اعتراض – بشكل احتيالي – بيانات محوسبة –غير عامة– أثناء نقلها إلى أحد أجهزة الحاسوب أو تُنقل منه أو داخله، وذلك من خلال وسائل تقنية.

---

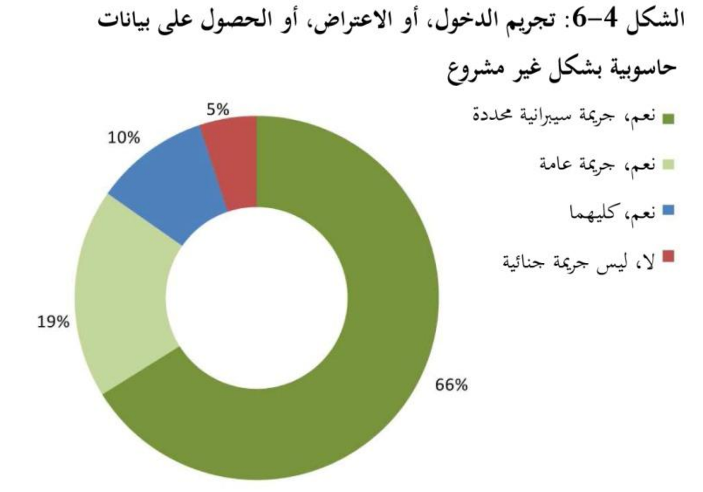
[1] Walden, I., 2007. *Computer Crime and Digital Investigations.* Oxford: OUP, p.184.

[2] مشروع اتفاقية الاتحاد الأفريقي (المادة 23/ج)، مشروع الميثاق النموذجي للكوميسا (المادة 21)، القانون النموذجي لدول كومنولث الدول المستقلة (المادة 8)، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية (المادة 3)، المشروع التوجيهي للجماعة الاقتصادية لدول غرب إفريقيا (المادة 6)، المقترح التوجيهي لدول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (المادة 6)، والنصوص التشريعية النموذجية للاتحاد الدولي للاتصالات السلكة واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات (المادة 6)، الاتفاقية العربية بشأن مكافحة جرائم المعلومات (المادة 7)، القانون النموذجي العربي لمواجهة الجريمة السيبرانية (المادة 8).

الأخرى تضطلع بتطبيق القوانين الحالية. ويتمثل السبب الوحيد وراء ذلك في حقيقة مفادها أن اعتراض البيانات الحاسوبية يمكن رؤيته سواء من وجه نظر سلامة البيانات أو حماية الخصوصية، أو أي منهما.

استفسر استبيان دراسة الجريمة السيبرانية عن الاعتراض غير المشروع للبيانات الحاسوبية في سياق اعتراض البيانات الحاسوبية أو الاطلاع عليها أو الحصول عليها، بيد أن الدراسة لم يحالفها التوفيق في جمع معلومات مباشرة بشأن الاعتراض غير المشروع بشكل منفصل. وبالرغم من ذلك، فإن الشكل 4-6 يظهر أن نسبة 85 في المائة من الدول المجيبة على الاستبيان المرافق لهذه الدراسة لديها أحكام تُجرم الاعتراض غير المشروع للبيانات الحاسوبية أو الاطلاع عليها أو الحصول عليها، في حين أن نسبة تزيد قليلا عن 65 في المائة من الدول تعتبر ذلك جريمة خاصة تتعلق بالفضاء السيبراني، حيث يظهر تحليل المصدر الرئيسي للتشريع في هذه الدول وجود اختلافات بين محل الجريمة والركن المادي لها.

الشكل 4-6: تجريم الدخول، أو الاعتراض، أو الحصول على بيانات حاسوبية بشكل غير مشروع



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال26. (رقم=59)

محل الجريمة – تعرف معظم الصكوك الدولية متعددة الأطراف والمعنية بمكافحة الجريمة السيبرنية الاعتراض القانوني بأنه نقل بيانات حاسوبية "غير عامة"، ومن ثم؛ يقتصر محل جريمة الاعتراض القانوني على المراسلات "الخاصة". ويشير هذا القيد إلى الطبيعة المقصودة لعملية الإرسال. على سبيل المثال؛ إحدى المراسلات التي تحمل طبيعة خاصة ولكن قد أرسلت للعامة عبر شبكة اللاسلكيات الدقيقة (Wi-Fi)، يمكن أن تكون هذه الرسالة محمية لأغراض الاعتراض غير القانوني، حَتّى لَوْ كانت عملية الارسال تمر عبر شبكة عامة.[1] ومن الملاحظ أن القانون النموذجي العربي لمواجهة الجريمة السيبرانية يعتبر الوثيقة الوحيدة فقط التي لا تحدّ مِن تجريم الإرسال إلى غير العامة (المادة 8). تتناول بعض الصكوك المتعددة الأطراف، أيضا بجانب عمليات الإرسال إلى غير العامة، مسألة اعتراض الاتصالات الكهرومغناطيسية، وهو مصطلح تم استخدامه لتوسيع نطاق الجريمة.[2]

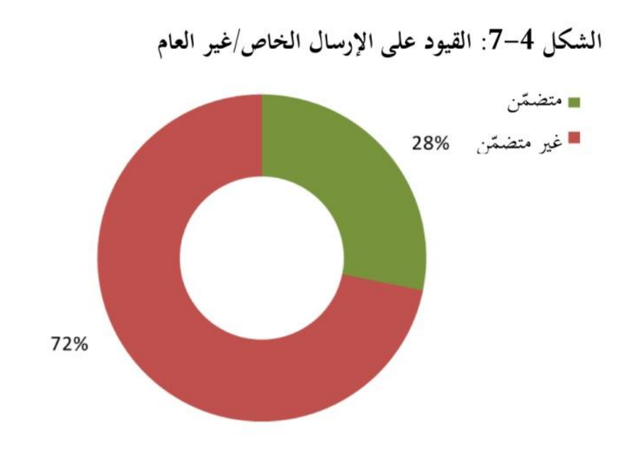
---

[1] أنظر على سبيل المثال، مجلس أوروبا 2001، التقرير التفسيري المرافق لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، سلسلة المعاهدات الأوروبية رقم 185.

[2] بما في ذلك القانون النموذجي لكومنولث الدول المستقلة، والنصوص التشريعية النموذجية للاتحاد الدولي للاتصالات السلكة واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المقترح التوجيهي لدول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

بينما تحدّ الأغلبية الساحقة من الصكوك متعددة الأطراف من تطبيق الاعتراض غير القانوني على انتقالات البيانات الحاسوبية، إلا أن تحليل التشريعات لـ 78 دولة يظهر أن نطاق الجريمة في العديد من الحالات لا يقتصر على نقل بيانات غير العامة، وذلك على المستوى الوطني. وفي هذا الشأن، يبين الشكل 4-7 أن ما يقل عن نسبة 30 في المائة من الدول التي تناولها التحليل تحدّ من الاعتراض غير المصرح به للمراسلات الخاصة أو المحمية. ولكن من الناحية العملية، ونظرا إلى التفسير الواسع لماهية "غير العامة"، فإنه من المرجح أن ذلك لا يمدّد من نطاق الجريمة بشكل كبير.

الشكل 4-7: القيود على الإرسال الخاص/غير العام



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=78)

الاعتراض غير المشروع: نموذج وطني لدولة في الأمريكتين

أي شخص يقوم عن علم وبدون عذر أو مبرر قانوني من خلال الوسائل التقنية باعتراض:

(أ) أي إرسال من أو إلى، أو داخل، أحد الأنظمة الحاسوبية التي لا تعتبر متاحة للجمهور، أو (ب) الاتصالات الكهرومغناطيسية التي تحمل البيانات الحاسوبية من نظام حاسوبي يعتبر في حالة إدانته مرتكبا لجريمة معاقب عليها بغرامة ____ أو بالسجن لمدة ____ أو كليهما معا.

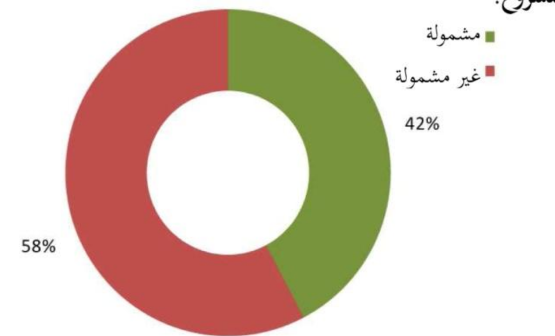
وتوجد مسألة إضافية تتعلق بمفهوم عملية "الإرسال"، حيث تعتبر البيانات في عداد الإرسال متى لم تصل إلى الوجهة النهائية – إما النظام أو المستلم المعني. كما يمكن اعتبار عملية نقل البيانات قد انتهت عندما تصل إلى نظام الحاسوب باعتباره الوجهة النهائية. وإلى جانب ذلك؛ يمكن اعتبار البيانات "في عداد الإرسال" عندما يتم تخزينها في النظام حتى يتحصل عليها المسْتَلِم المعني. فمن الملاحظ أن أي صك متعدد الأطراف لا يقدم تَوْجِيها بشأن نقطة النهاية لعملية الإرسال، حيث تعتبر التمييز من الأمور الهامة فيما يتعلق بالتخزين المؤقت للبيانات الذي يحدث عندما تُرسل البيانات الحاسوبية باستخدام بروتوكولات تعمل على أساس "التخزين والإرسال".[1]

لقد تناولت العديد من الدول هذه المسألة في التشريعات الوطنية. فعلى سبيل المثال؛ إحدى الدول في أوقيانوسيا، تتبنى حكما قانونيا يستبعد *"المراسلة المخزنة على أساس انتقالي كجزء من وظيفة لا تتجزأ من التكنولوجيا المستخدمة في نقلها"* من المراسلة المخزنة والمحددة. وبالتالي، فإن مثل هذه البيانات يمكن إدراجها ضمن نطاق جريمة الاعتراض غير القانوني للبيانات الحاسوبية.

[1] Walden, I., 2007. *Computer Crime and Digital Investigations*. Oxford: OUP, p.185

الأفعال المشمولة – تحصر الصكوك متعددة الأطراف الركن المادي لجريمة الاعتراض غير القانوني على الأفعال التي تُرتكب باستعمال وسائل تقنية، باستثناء صك واحد فقط لم يتعرض لهذا الأمر.[1] ويمثل هذا المطلب طبقا للتقرير التفسيري المرافق لاتفاقية مجلس أوروبا بشأن الجريم السيبرانية شرطا مقيدا لتجنب المغالاة في عملية التجريم.[2] وبالرغم من ذلك، فإن التَحْدِيد لا ينعكس دائما في النُهُج الوطنية. ويظهر الشكل 4-8 أن أكثر من نصف الدول – في جميع مناطق العالم – التي خضعت تشريعاتها للتحليل لم تدرج الوسائل التقنية كعنصر من العناصر المكونة للركن المادي لجريمة الاعتراض غير المشروع.


الشكل 4-8: هل الوسائل التقنية مشمولة كعنصر لجرائم الاعتراض غير المشروع؟



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=78)

الركن المعنوي – تشترط عادة الصكوك متعددة الأطراف أن تتوافر نية الفعل المتعمد عند ارتكاب جريمة الاعتراض غير المشروع، فعلى سبيل المثال؛ تقتضي اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية أنه بإمكانية الدول الأطراف أن تحد من الأفعال التي تشكل جريمة الاعتراض القانوني في الحالات التي ارتكبت فيها، والمقترنة بتوافر نية الاحْتِيَالِيّة لدى الجاني. وقد أظهر استعراض التشريعات الوطنية أن هناك دولا قليلة تشترط نية إضافية، بينما ترى دول أخرى أن نية ارتكاب جريمة الاعتراض غير القانونية تصاحبها نية ارتكاب جرائم أخرى دون الفصل بين النيتين. فعلى سبيل المثال، تجرم إحدى دول أوروبا الشرقية الاعتراض غير القانوني للبيانات الحاسوبية فقط إذا كان الهدف ارتكاب جرائم حاسوبية محددة. إلى جانب ذلك، تعتبر بعض الدول وجود نية

التدخل غير المشروع: قرار الاتحاد الأوروبي بشأن الهجمات على أنظمة المعلومات

المادة 4 – التدخل غير المشروع في البيانات

يجب على كل دولة عضو أخذ التدابير اللازمة لضمان أن حذف نظم المعلومات بشكل عمدي أو الإضرار بها أو إتلافها أو تغييرها أو طمسها أو ما يجعل الوصول إليها متعذرا بلوغه، يعتبر جريمة جنائية معاقب عليها متى ارتكبت بدون وجه حق، على الأقل للحالات التي لا تعتبر بسيطة.

التدخل غير المشروع: اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

المادة 5 – التدخل في نظام

يجب على كل طرف أن يعتمد تدابير تشريعية وتدابير أخرى قد تكون ضرورية ليجرم بموجب قانونه الداخلي، عندما ترتكب عمدا، عرقلة أداء نظام حاسوبي بشكل خطير دون وجه حق، وذلك عن طريق إدخال بيانات حاسوبية أو إرسالها أو إلحاق ضرر بها أو مسحها أو إتلافها أو تغييرها أو طمسها.

---

[1] المادة (8) من الاتفاقية العربية لمكافحة جرائم المعلومات

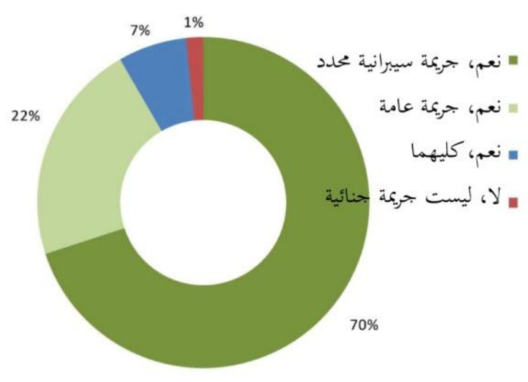
[2] مجلس أوروبا، 2001. التقرير التفسيري المرافق لاتفاقية مجلس أوروبا بشأن الجرائم السيبرانية، سلسلة المعاهدات الأوروبية رقم 185.

إضافية بمثابة شرط مشدد للعقوبة. وفي هذا الصدد، تعتبر دولتان من دول أوروبا الغربية أن الاعتراض غير المصرح به بقصد تحقيق مكاسب مالية بمثابة ظرف لتشديد العقوبات.

التدخل غير المشروع في نظام حاسوبي أو بيانات حاسوبية

يهدد التدخل غير المشروع في أنظمة الحاسوب أو البيانات الحاسوبية سلامة وتوافر بيانات الحاسوب، علاوة على التشغيل الصحيح لبرامج الحاسوب وأنظمته. ونظرا للطبيعة غير المادية للبيانات الحاسوبية، فإن العديد من نظم التشريعات الوطنية تعجز عن تمديد أحكام القانون الجنائي التقليدية التي تتعامل مع الممتلكات المادية أو تديرها لتشمل التدخل غير القانوني في البيانات الحاسوبية.[1] ومن ثم، فإن أغلب الصكوك متعددة الأطراف تتضمن جرائم خاصة تتعلق بالتدخل غير القانوني في أنظمة الحاسوب أو البيانات الحاسوبية.

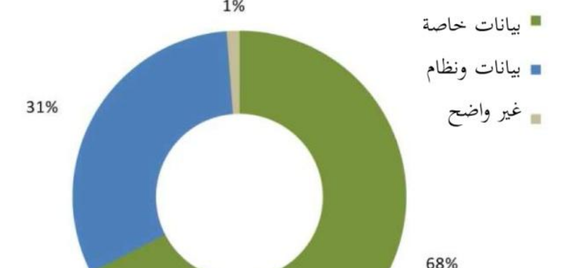
الشكل 4-9: تجريم التدخل غير المشروع في البيانات أو الإضرار بنظام



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال27 (رقم=60)

وعلى المستوى الوطني، يظهر الشكل 4-9 أن أكثر من 90 في المائة من الدول المجيبة على الاستبيان الخاص بهذه الدراسة لديها جريمة جنائية تتناول التدخل غير القانوني في أنظمة الحاسوب أو البيانات الحاسوبية، كما أفادت نسبة سبعين في المائة من هذه الدول بأن لديها جرائم خاصة بالفضاء السيبراني. أفادت نسبة 7 في المائة من الدول المجيبة أن كلا من الجريمة العامة والجرائم الخاصة بالفضاء السيبراني تتناول هذا الفعل. وتظهر مراجعة المصدر الرئيسي الخاص بتشريعات 83 دولة، أن هناك اختلافات في التشريعات الوطنية تتعلق بشروط محل الجريمة والركن المعنوي، والظروف *المشددة المرافقة* للجريمة.

الشكل 4-10: محل التدخل في البيانات



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=83)

محل الجريمة – تشترط أغلب الصكوك متعددة الأطراف اعتماد أحكام منفصلة لتجريم التدخل غير القانوني في أنظمة الحاسوب أو البيانات الحاسوبية،[1] بيد أن

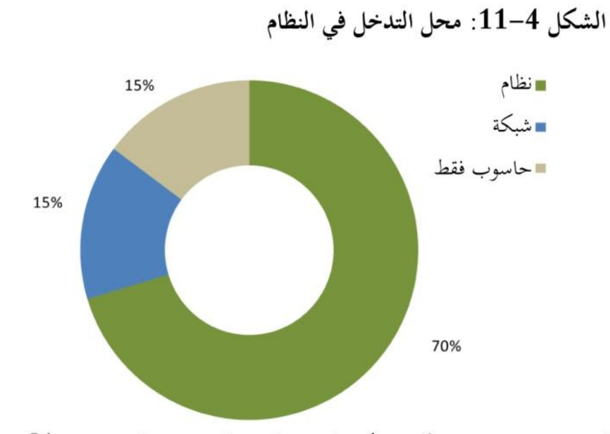
---

[1] Sieber, U., 2008. Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. *In:* Delmas-Marty, M., Pieth, M. and Sieber, U., (eds.) *Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law. Collection de L'UMR de Droit Comparé de Paris.* Vol. 15. Paris: Société de législation comparée.

القانون العربي النموذجي لمواجهة الجريمة السيبرانية يعتبر الصك الوحيد الذي يتضمن الجمع بين الرأيين دون أحكام منفصلة.[2]

وقد اتضح من خلال استعراض التشريعات الوطنية أن أغلبها تتضمن أحكاما منفصلة تتصدى للتدخل غير القانوني في أنظمة الحاسوب أو البيانات الحاسوبية. ومع ذلك، فإن ما يقرب من 30 في المائة من الدول التي خضعت لعملية التحليل ليس لديها أحكام منفصلة للجرائم بشكل واضح، إلى جانب أن هذه النسبة من الدول تجرم التدخل غير القانوني في البيانات فقط عندما يؤثر هذا التدخل على الأداء الوظيفي لنظام الحاسوب. بينما يكون ذلك هو الأمر المعمول به عمليّا، إلا أنه من الممكن أن يترك النهج المتبع ثغرات في عملية تجريم التدخل غير القانوني في البيانات بمفردها. وبالرغم من ذلك، لا يزال القانون الجنائي العام يضطلع بتناول هذه المسألة في بعض الدول. فعلى سبيل المثال ؛ تستخدم إحدى دول الأمريكتين، حكما عامّا بشأن تدمير أو إلحاق الخلل "بالسلع"، حيث تدرج البيانات الحاسوبية ضمن تعريف "السلع".

الشكل 4–11: محل التدخل في النظام



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=81)

وفيما يتعلق بعنصر *النظام* في التدخل غير المشروع، فإن تحليل الأحكام المتاحة يظهر أن معظم القوانين الوطنية غالبا ما تتناول "نظم" الحاسوب. ومع ذلك، ربطت ما يقرب من نسبة 30 في المائة من الدول الجريمة إما "بالشبكات" أو "أحد أجهزة الحاسوب". ومن ثم، فإن هذا قد يحدّ من التجريم، نحو استبعاد الحالات التي لا يعتبر فيها الحاسوب المتعرض للضرر من قبيل الشبكية، أو الحالات التي تعاني فيها عدة أجهزة، بما في ذلك موجهات الشبكة، من التدخل، وذلك من خلال هجوم البرمجيات الخبيثة أو حجب الخدمة الموزعة، على سبيل المثال.

الأفعال المشمولة – تتناول الصكوك متعددة الأطراف تجريم عدد من الأفعال المختلفة التي تشكل جريمة التدخل غير القانونية في البيانات، ولا يتضمن ذلك فقط إلحاق الضرر بالبيانات، بل يمتد ليشتمل على "حذف" البيانات أو "إتلافها" أو "تغييرها" أو "طمسها"، وحتى "إدخالها"، ومن ثم تتوفر حماية سلامة البيانات بمدلول

---

[1] مشروع اتفاقية الاتحاد الأفريقي، المواد 19/ج، 20/ج، مشروع ميثاق الكوميسا المادة 20/ب، القانون النموذجي لدول اتحاد الكومنولث الماد65، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المادة4، المشروع التوجيهي للجماعة الاقتصادية لدول غرب إفريقيا المادتان 5، و7، قرار دول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات المادة 3 مقترح توجيهي لدول الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات المادة 4، النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات السلكة واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات المادة 7، الاتفاقية العربية بشأن مكافحة جرائم المعلومات المادة 8.

[2] القانون النموذجي للدول العربية المادة 6.

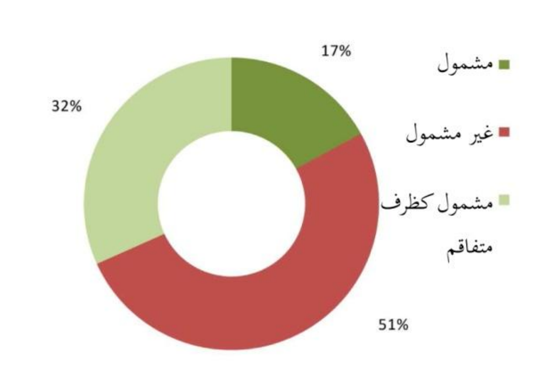
واسع النطاق. ويظهر الشكل 4-12 أن أغلبية القوانين الوطنية، التي خضعت للتحليل، تتناول الأفعال المتعلقة بإتلاف البيانات أو حذفها، أو تعديلها. وفي هذا الصدد؛ فإن نسبة 35 في المائة فقط من الدول أدرجت "إدخال" البيانات في الأحكام المعنية بتجريم التدخل غير القانوني. أما فيما يتعلق "بطمس" البيانات؛ فإن ما يزيد عن نسبة 40 في المائة من الدول تناولت هذا الفعل. بيد أن نسبة 12 في المائة فقط من الدول التي تجرم عملية "إرسال" البيانات بموجب الأحكام التي تجرم التدخل غير القانوني. فمن المتوقع تجريم "إرسال" البيانات في الدول في حالة إذا تم إدماج التدخل غير القانوني في البيانات والنظام الحاسوبي في حكم واحد، تأسيسا على أن إرسال البيانات له تأثير على النظام الحاسوبي. ومع ذلك؛ يظهر التحليل عدم وجود ارْتِبَاط بين ذلك وذاك. وجدير بالذكر؛ أن الدول التي تجرم التدخل غير القانوني بأحكام منفصلة، تدرج أيضا عملية إرسال البيانات ضمن قائمة الأفعال المحظورة.

الشكل 4-12: العناصر المكونة للتدخل غير المشروع في البيانات

إضرار/حذف	95%
تغيير	98%
طمس	43%
إدخال	35%
إرسال	12%

المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=83)

الشكل 4-13: هل الإضرار مشمول كعنصر ضروري للتدخل في البيانات؟



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=83)

تجيز بعض الصكوك متعددة الأطراف إبداء تحفظات بشأن الآثار الناجمة عن التدخل غير القانوني في البيانات الحاسوبية. فعلى سبيل المثال؛ تنص اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية على إمكانية قصر تجريم التدخل غير القانوني في البيانات في حالات الضرر الجسيم،[1] كما يمنح قرار الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات حرية التجريم من عدمه للحالات البسيطة.[1]

التدخل في النظام: مثال وطني من دولة في جنوبي أفريقيا

الإضرار بنظام حاسوبي أو حجب الدخول إليه

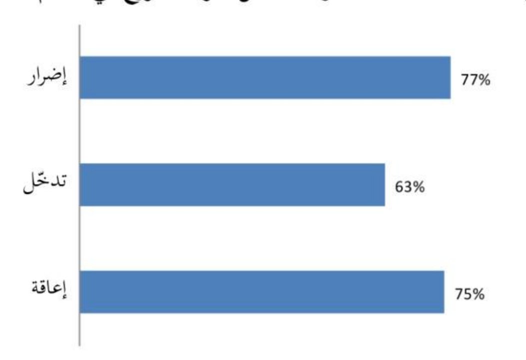
أي شخص يضطلع بدون تفويض قانوني أو عذر قانوني بأي فعل من شأنه أن يسبب بشكل مباشر أو غير مباشر (أ) تراجع أحد الأنظمة الحاسوبية أو تَعَطّل أو عرقلة تشغيلها، أو (ب) يحول دون الوصول إليه أو إتلاف أي من البرامج أو البيانات المخزنة، يعتبر مرتكبا لجريمة، ويعاقب –في حالة إدانته– بغرامة لا تتجاوز _____ والسجن مع الأشغال الشاقة لمدة لا تتجاوز _____ سنة.

[1] المادة (4) من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

ويبين الشكل 4–13 أن نسبة 17 في المائة فقط من الدولة التي خضعت للتحليل تدرج الضرر أو الخسارة كعنصر ضروري لقيام جريمة التدخل غير القانوني في البيانات الحاسوبية. كما أن نسبة 30 في المائة من الدول تدرج الضرر الناجم عن التدخل غير القانوني في البيانات كأحد الظروف المشددة للعقوبة. هذا، ولا تشير نصف القوانين الوطنية في أحكامها ذات الصلة إلى الضرر برمته الناجم عن التدخل غير االمشروع في البيانات.

وبنفس نمط التدخل غير المشروع في البيانات، فإن أنظمة الحاسوب قد تتعرض للإتلاف بطرق مختلفة، وقد يتم ذلك على سبيل المثال عن طريق إرسال أو تغيير أو حذف البيانات الحاسوبية، أو من خلال التدخل الكهرومغناطيسي أو عن طريق قطع إمدادات الطاقة عن النظام. وعادة ما تتضمن الأحكام الواردة في الصكوك متعددة الأطراف والمعنية بالتدخل غير القانوني في النظام "حذف أو تغير أو إرسال البيانات"، أو أي وسيلة أخرى من وسائل "التدخل" في البيانات. وبالرغم من ذلك، فإن التعريفات الواسعة الواردة في القانون النموذجي لدول الكومنولث والنصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/مجموعة الكاريبي/الاتحاد الكاريبي للاتصالات التي لا تتضمن التلاعب بالبيانات فقط وإنما تتضمن أيضا قطع التيار الكهربائي عن أحد الأنظمة الحاسوبية، وكذلك أي وسيلة من وسائل إفساد النظم الحاسوبية أو التدخل فيها.[2]

الشكل 4–14: الأفعال المكونة للتدخل غير المشروع في النظام



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=81)

ويبين الشكل 4–14: أن أغلبية التشريعات الوطنية التي خضعت للتحليل أدرجت أفعال "الإتلاف/الإضرار"، و"التدخل"، و"الإعاقة/الإيقاف" ضمن أحكامها. وقد تمت ملاحظة اتجاهين تشريعيين، أولهما يتبنى بشكل واسع استخدام مصطلح "الإيقاف بأي وسيلة" مما يولد قاعدة عريضة من تجريم التدخل في الأنظمة الحاسوبية، أما الاتجاه الثاني قائم على ارْتِباط الأحكام المعنية للتدخل في الأنظمة بالأحكام المنوط بها التدخل غير القانوني، مما يشكل ذلك قاعدة ضيقة من التجريم.

الركن المعنوي للجريمة – يشترط العديد من الصكوك متعددة الأطراف والمنوط بها مكافحة الجريمة السيبرانية أن تتوافر نية "الفعل المتعمد"، أو نية "القصد الاحتيالي" لقيام جريمة التدخل غير القانوني في النظم أو

---

[1] المادة (3) قرار الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات

[2] المادة 7 من القانون النموذجي لدول الكومنولث والمادة 10/3 من النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/موجوعة الكاريبي/الاتحاد الكاريبي للاتصالات

البيانات الحاسوبية.[1] بيد أن القانون النموذجي العربي لمواجهة الجريمة السيبرانية لم يذكر النية في الأحكام المعنية بالتدخل في البيانات، ومع ذلك، فإنه يشترط وجود غرض محدد يهدف إلى توقف سير أداء النظام أو البيانات.[2] غير أن القانون النموذجي لدول اتحاد الكومنولث قد حذا نهجا مختلفا حيث نص صراحة على تجريم أفعال التدخل المرتكبة "بتهور".[3] وهذا يولد بشكل خاص قاعدة عريضة من التجريم في ضوء حقيقة مؤداها أن التدخل غير المتعمد في البيانات الحاسوبية أو عملية تشغيل نظم الحاسوب غالبا ما تكون أيسر من استهداف الممتلكات أو الأغراض في العالم المادي.[4] وباستقراء الواقع، فإن ستة دول فقط من أصل 81 دولة من الدول التي خضعت أحكامها المعنية بالتدخل للاستعراض اتبعت هذا النهج، كما تجرم أفعال التدخل في البيانات سواء كان ذلك "بتهور" أو بإهمال". وجدير بالذكر أن أغلبية هذه الدول ليست عضوا في دول اتحاد الكومنولث، ولكن وجدت هذه الدول في أمريكا الجنوبية، وأوروبا الغربية، وأفريقيا.

التدخل غير المشروع في البيانات: مثال وطني من دولة في جنوب–شرق آسيا

التعديل بدون تصريح لمحتويات أي حاسوب

(1) يعتبر أي شخص مرتكبا لجريمة إذا قام بدون تصريح بأداء فعل يعلم أن من شأنه تعديل محتويات أي حاسوب.

(2) ولأغراض هذه المادة، ليس من الأهمية أن يكون الفعل محل الجريمة موجها إلى–

(أ) أي برنامج أو بيانات محددة؛

(ب) أي نوع من البرامج أو البيانات؛ أو

(ج) برنامج أو بيانات موجودة في أي حاسوب معين.

(3) ولأغراض هذه المادة، ليس من الأهمية أن يكون التعديل غير المصرح به مؤقتا أو بصفة دائمة.

ولأغراض هذا القانون، يعتبر في نطاق تعديل محتويات أي حاسوب، إذا كان من خلال تشغيل أي مهام وظيفية للحاسوب المعني أو حاسوب من الحواسيب الأخرى –

(أ) أي برامج أو بيانات موجودة في الحاسوب قد تم تغييرها أو محوها؛

(ب) أي برامج أو بيانات يتم إضافتها أو إدخالها في محتويات الحاسوب المعني؛

(ج) أي فعل يحدث يكون من شأنه تعديل عملية التشغيل العادي لأي حاسوب؛

وأي فعل يساهم في إحداث هذا التعديل ينبغي اعتباره متسببا في ضرر.

الظروف المشددة للعقوبة –

لا تشترط الصكوك متعددة الأطراف والمنوط بها مكافحة الجريمة السيبرانية فِي أَكْثَرِ الْأَحْيَان تشديد العقوبات المفروضة لجرائم التدخل غير القانوني في البيانات، بيد أن هناك استثنائين من هذه الصكوك؛ ومنها المشروع التوجيهي للجماعة الاقتصادية لدول

---

[1] مشروع اتفاقية الاتحاد الأفريقي المادة 19/ج، 20/ج، مشروع القانون النموذجي لدول الكوميسا المادة 20/ب، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المادة 4، المشروع التوجيهي للجماعات الاقتصادية لدول غرب أفريقيا المادة 5، 7، قرار الاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات المادة رقم 3، المشروع التوجيهي للاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات المادة رقم 4، النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/موجوعة الكاريبي/الاتحاد الكاريبي للاتصالات المادة 7، الاتفاقية العربية بشأن مكافحة جرائم المعلومات المادة8.

[2] القانون النموذجي العربي لمواجهة الجريمة السيبرانية، المادة6.

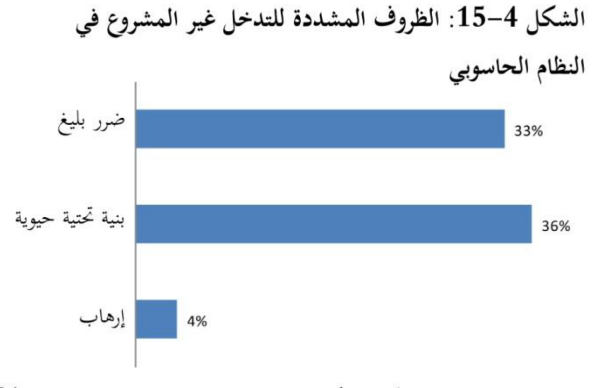
[3] القانون النموذجي لدول اتحاد الكومنولث المادة 6،

[4] De Hert, P., Fuster, G. and Koops, B. J., 2006. Fighting cybercrime in the two Europes. The added value of the EU framework decision and the Council of Europe Convention. *International Review of Penal Law*, 77:6.

غرب أفريقيا الذي ينص على تشديد العقوبة متى اقترنت بنية إحداث ضرر جسيم أو تهديد السلامة العامة، أو إذا كانت مقترنة بتعطيل البنية التحتية للمنشآت الحيوية أو للأغراض الإرهابية.[1] أما الاستثناء الثاني من هذه الصكوك، يتمثل في المشروع التوجيهي للاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات (كما في حالة النفاذ غير المشروع) الذي طالب الدول بأن تقر الظروف المشددة في حالة تورط منظمات إجرامية، أو إذا ارتكبت الجريمة من خلال استعمال أدوات مصممة للهجوم على عدد من نظم المعلومات الهامة، أو عند إخفاء الهوية الحقيقة للجاني.[2]

العديد من الدول على المستوى الوطني تلحق تجريم التدخل في البيانات بظروف مشددة تستدعي عقوبات أشد. ويظهِر الشكل 4-15 أن غالبية الدول عادة ما تشدد العقوبات متى تسبب التدخل في "ضرر بَلِيغ" أو إذا ارتبط التدخل "بالبنية التحتية الحيوية". بيد أن عددا قليلا من الدول التي خضعت تشريعاتها للاستعراض تأخذ أيضا بالظروف المشددة للعقوبة متى ارتبط التدخل بالإرهاب، كما أن عددا أقَلّ من القوانين تعتبر ارتكاب الفعل في شكل منظم وبهدف اكتساب ملكية من قبيل الظروف المشددة للعقوبة. وأخيرا، قام عدد قليل من الدول أيضا بوضع حمايات إضافية لأنواع معينة من البيانات. فعلى سبيل المثال، وضعت إحدى الدول الآسيوية ظروفا مشددة للعقوبة متى اقترن التدخل ببيانات تتعلق بالسجلات الطبية أو الرعاية الصحية.

الشكل 4-15: الظروف المشددة للتدخل غير المشروع في النظام الحاسوبي



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=81)

أدوات إساءة استعمال الحواسيب

لقد أصبح استعمال البرمجيات والأدوات الأخرى في ارتكاب الجرائم إلى جانب اختراق كلمات المرور والكلمات السرية للدخول الخاصة بالضحية في البيئة الرقمية بمثابة مادّة غير مشروعة في الأسواق السِرّيّة للجريمة السيبرانية.[3] بيد أن تجريم هذه "الأدوات المستخدمة في ارتكاب أعمال إجرامية" يواجه عددا من التحديات، ليست أقل من الحدود المرنة بين "الإعداد للجريمة" و"الشروع" في ارتكابها، فضلا عن إشكالية "الاستخدام المزدوج" لهذه الأدوات، والتي قد تستخدم إما في ارتكاب أعمال إجرامية أو أعمال غير مؤذية. وبالرغم من ذلك، فقد وضعت الصكوك متعددة الأطراف والمنوط بها مكافحة الجريمة السيبرانية جرائم مماثلة لتلك الموجودة في

---

[1] القانون النموذجي للجماعة الاقتصادية لدول غرب أفريقيا، المادة 20، الفقرات ج، د، هـ، و.

[2] المشروع التوجيهي للاتحاد الأوروبي بشأن الهجمات ضد نظم المعلومات المادة 10

[3] Europol, 2011. *Threat assessment (abridged). Internet facilitated organised crime*. iOCTA. File No.: 2530–264. The Hague. 7 January. Available at: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf ; Fallmann, H., Wondracek, G. and Platzer, C., 2010. *Covertly probing underground economy marketplaces*. Vienna University of Technology

السوابق القضائية المعنية بمكافحة الجريمة "التقليدية"، والتي تجرم الأدوات المستخدمة في ارتكابها مثل "الأدوات المستخدمة في جريمة السطو المسلح".[1] فعلى سبيل المثال، تفيد المذكرة التفسيرية المرافقة لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية بأن الأَساس المَنْطِقِيّ لتجريم أدوات إساءة استعمال الحاسوب يتمثل في استهداف الأفعال السابقة للجريمة مثل "القرصنة"، بالإضافة إلى منع إنشاء أسواق سوداء لهذه المواد.[2] ومن أجل منع المغالاة في تجريم حيازة أدوات إساءة استعمال الحاسوب غير معروف الهدف من حيازتها أو حيازتها بنية مشروعة، فإن الصكوك الدولية والإقليمية عادة ما تتطلب توافر نية خاصة لاستخدام هذه الأدوات لأغراض جنائية.

يظهر الشكل 4-16 أن أكثر من نصف الدول المجيبة على الاستبيان الخاص بهذه الدراسة يجرمون أدوات إساءة استعمال الحاسوب، وغالبا من خلال استعمال إحدى الجرائم الخاصة بالفضاء السيبراني. ومع ذلك، فإن حوالي نسبة 20 في المائة من الدول المجيبة لا تجرم أدوات إساءة استعمال الحاسوب. وقد أظهر تحليل المصدر الرئيسي لتشريع 70 دولة، أن هذه التشريعات تتضمن أحكاما تكشف عن مناهج متنوعة لتحديد ماهية محل الجريمة والركن المادي والركن المعنوي المطلوبين لقيام جريمة أدوات إساءة استعمال الحاسوب.

أدوات إساءة استعمال الحاسوب: القانون النموذجي للكومنولث

المادة 9(1) – الأدوات غير المشروعة

يعتبر أي شخص مرتكبا لجريمة، إذا:

(أ) قام عمدا أو بتهور، وبدون عذر أو مبرر قانوني؛ بإنتاج أو بيع أو شراء من أجل الاستخدام، أو استيراد أو تصدير أو توزيع، أو يتيح بوسائل أخرى:

(1) أحد الأجهزة، بما في ذلك برنامج حاسوبي، التي قد صممت أو تم تكييفها لأغراض ارتكاب جرائم على النحو الوارد في المواد 5، 6، و7، أو المادة 8؛ أو

(2) كلمات مرور أو رموز دخول لأحد الحواسيب أو البيانات المماثلة التي تمكن من اختراق النظام كليا أو جزئيا؛

بنية استخدامه من قبل أي شخص لغرض ارتكاب إحدى الجرائم الواردة في المواد 5، 6، و7، أو المادة 8؛ أو

(ب) كانت أي من المواد المذكورة في الفقرة الفرعية (1) أو (2) في حيازته، وذلك بنية استخدامه من قبل أي شخص لغرض ارتكاب إحدى الجرائم الواردة في المواد 5، 6، و7، أو 8.

(ج) أي شخص يدان بارتكاب أي من الجرائم الواردة في هذه المادة، يعاقب بالسجن لمدة لا تزيد عن _____، أو بغرامة لا تتجاوز _____، أو بالعقوبتين معا.

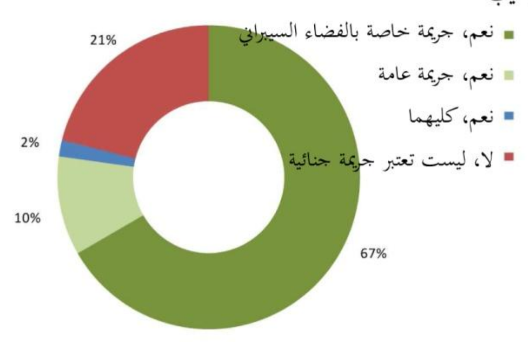
محل الجريمة – تتضمن الصكوك متعددة الأطراف والمنوط بها مكافحة الجريمة السيبرانية أحكاما تتعلق بنوعين من أدوات إساءة استخدام الحواسيب: (1) البرمجيات والأجهزة، (2) كلمات المرور والرموز التي تمكّن من الوصول إلى الأنظمة الحاسوبية أو البيانات الحاسوبية. بيد أن تسعة من هذه الصكوك تتضمن تجريم كل من البرمجيات والرموز. ومع ذلك، يوجد صك واحد (اتفاقية دول كومنولث الدول المستقلة) يتضمن تجريم استعمال

[1] See, Fletcher, G., 1978. *Rethinking Criminal Law*. Boston: Little, Brown & Co. pp.199-202.

[2] مجلس أوروبا 2001، المذكرة التفسيرية المرافقة لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، سلسلة المعاهدات الأوروبية رقم 185

وتوزيع البرمجيات الخبيثة، ومن ثم؛ تستبعد الاتفاقية الأجهزة والرموز من نطاق محل التجريم.[1] ومن الجدير بالذكر، أنه في حالة استعمال مصطلح "أجهزة"، فإن ذلك يتناول كلا من الأجهزة والبرمجيات.

الشكل 4–16: تجريم إنتاج أو توزيع أو حيازة أدوات إساءة استخدام الحواسيب

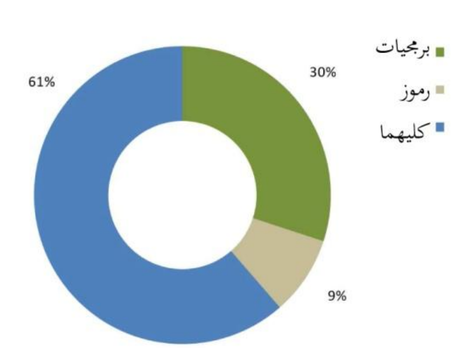


المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 28. (رقم=57)

وإلى جانب الأحكام التي تتناول الأدوات المستخدمة في ارتكاب جريمة سيبرانية بشكل عام، فإن بعضا من الصكوك متعددة الأطراف تتناول أيضا الأجهزة والأدَوات المستخدمة في ارتكاب جرائم محددة. فعلى سبيل المثال؛ يتضمن قرار دول الاتحاد الأوروبي بشأن الاحتيال وتزوير وسائط الدفع غير النقدية تجريم "الأجهزة"، و"الأدوات"، "برامج الحاسوب" وأي وسائل أخرى تم تكييفها بشكل استثنائي لارتكاب أي من الجرائم المنصوص عليها في الفقرة (ب) من المادة 2" (تزوير وتزييف وسائط الدفع لاستعمالها بشكل احتيالي)، فضلا عن "برامج الحاسوب، لأغراض ارتكاب أي من الجرائم المنصوص عليها في المادة 3" (الجرائم ذات الصلة بالحاسوب، وبخاصة الاحتيال الحاسوبي).[2]

تظهر النهج الوطنية بشأن تعيين محل جرائم الأجهزة غير المشروعة نوعا من التَعَدّد. ويبين الشكل 4–17 أن أغلبية الدول التي خضعت تشريعاتها للاستعراض تُجرم كلّا من الأجهزة والرموز. ومع ذلك، فإن عددا كبيرا من القوانين الوطنية تحصر التجريم إما في الأجهزة بمفردها (30 في المائة)، أو كلمات السر والرموز بمفردها (حوالي 10 في المائة). بيد أن تعيين محل الجريمة في بعض الدول الأخرى قد اتخذ منهجا مغايرا، حيث تجرم استحداث فيروسات حاسوبية ونشرها بدلا من البرمجيات والرموز أو بجانبهما. كما أن العديد من الدول تجرم أيضا الأفعال ذات الصلة بحيازة أو توزيع "أدوات تستعمل للاحتيال الحاسوبي"، حيث إن الأحكام التي تجرم هذا النوع بدت واضحة في 12 دولة من أصل 70 دولة من الدول التي خضعت للتحليل.

الشكل 4–17: أنواع أدوات إساءة استخدام الحواسيب



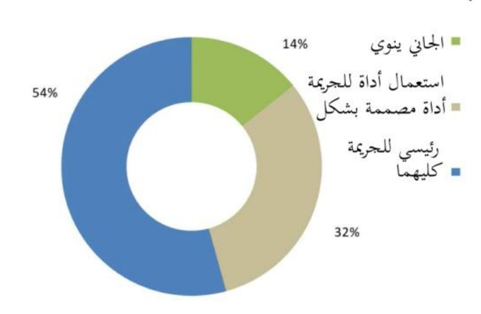
المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=70)

[1] اتفاقية دول كومنولث الدول المستقلة، المادة 2(1/ب).

[2] القرار الإطاري لمجلس الاتحاد لأوروبي 2001/413/JAI of، 28 آيار/مايو 2001، (قرار الاتحاد الأوروبي بشأن مكافحة الاحتيال وتزوير وسائط الدفع غير النقدية).

وهناك سمة أخرى هامة للجريمة تتمثل في ماهية الغرض من الأداة. فعلى سبيل المثال؛ اشترطت أغلب الصكوك متعددة الأطراف أن يكون "سوء استخدام أحد الأجهزة" قد تم تصميمه بشكل أساسي لارتكاب إحدى الجرائم، وإلى جانب ذلك، فإن العديد من الصكوك تشترط أيضا أن تتجه نية الجاني نحو استعمال الأداة لارتكاب إحدى الجرائم. ومع ذلك، يوجد صكان من الصكوك متعددة الأطراف (اتفاقية الاتحاد الأوروبي واتفاقية كومنولث الدول المستقلة) يتناولان فقط ماهية الغرض من الأداة، دون نية الجاني. ويظهر الشكل 4-18 أن ما يزيد عن نسبة 50 في المائة-على المستوى الوطني-من الدول التي خضعت تشريعاتها للاستعراض تشترط كلا من الأداة المصممة بشكل رئيسي لارتكاب جريمة ونية الجاني المتجهة نحو استعمال هذه الأداة.[1] ومع ذلك، فإن بعض النُهُج الوطنية تركز فقط – بشكل منفصل – على ماهية الغرض من الأداة، أو ماهية نية الجاني لوحده.

الشكل 4-18: النية المطلوبة لجرائم أدوات إساءة استخدام الحواسيب



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=70)

أدوات إساءة استعمال الحاسوب: مثال وطني من دولة في أوقيانوسيا

جرائم الحاسوب والاتصالات-

(1) لا يجوز لأي شخص: ...

(و) أن يقوم عمدا وبدون حق وبشكل احتيالي أو بنية غير مشروعة؛ باستعمال، حيازة، إنتاج، بيع، شراء من أجل الاستخدام، استيراد، توزيع أو إتاحة أو الشروع في استعمال أو حيازة أو إنتاج أو بيع أو شراء من أجل الاستخدام أو استيراد أو توزيع أو إتاحة أحد الأجهزة، بما في ذلك على سبيل المثال لا الحصر، أحد برامج الحاسوب، لأغراض ارتكاب أي من الجرائم الواردة في الفقرات (أ)، (ب)، (ج)، (د)، أو (هـ)؛

(ز) أن يقوم عمدا وبدون حق وبشكل احتيالي أو بنية غير مشروعة؛ باستعمال، حيازة، إنتاج، بيع، شراء من أجل الاستخدام، استيراد، توزيع أو إتاحة أو الشروع في استعمال أو حيازة أو إنتاج أو بيع أو شراء من أجل الاستخدام أو استيراد أو توزيع أو إتاحة كلمات المرور لأحد الحواسيب أو رموز الدخول أو البيانات المماثلة التي تمكن من الدخول بشكل كلي أو جزئي إلى إحدى شبكات الاتصالات بهدف استخدام هذه الشبكة أو النظام لأغراض ارتكاب أي من الجرائم الواردة في الفقرات (أ)، (ب)، (ج)، (د)، أو (هـ)؛ ...

(2) كل شخص يتصرف بما يخالف أيا من الأحكام الواردة في البند (1) يرتكب جريمة، ويعاقب بالعقوبات المنصوص عليها في المادة ____.

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة (استعراض التشريعات).

الأفعال المشمولة – تتضمن الصكوك متعددة الأطراف مجموعة كبيرة من الأفعال ذات الصلة بأدوات إساءة استخدام الحاسوب، ومنها؛ "إنتاج"، "بيع"، "استيراد"، "توزيع"، "نشر"، "عرض"، "نقل"، و"إتاحة" هذه الأدوات. وعلى النحو المبيّن في الشكل 4-19؛ فإن تحليل القوانين الوطنية يظهر أن ما يزيد عن نسبة 80 في المائة من الدول تجرم عملية "نَشْر" هذه الأدوات. كما تضطلع نسبة 65 في المائة من الدول بتجريم "حيازة" أدوات إساءة استخدام الحاسوب. بالإضافة إلى ذلك، فإن بعض القوانين الوطنية تجرم أيضا الأفعال التي ترد في الصكوك الدولية أو الإقليمية، والتي يمكن اعتبارها بمثابة أحكام تتعلق بأدوات إساءة استخدام الحاسوب. فعلى سبيل المثال؛ تجرم العديد من دول منطقة الكاريبي الفعل المتعلق "بالكشف غير المصرح به" عن كلمات السر ورموز الدخول للحواسيب.

الشكل 4-19: أفعال متعلقة بأدوات إساءة استخدام الحاسوب



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=70)

رسائل البريد الإلكتروني الطفيلي (Spam)

تشير التقديرات إلى أن الرسائل الإلكترونية الطفيلية تشكل حوالي 70 في المائة من حركة مرور البريد الإلكتروني عبر الإنترنت، في منتصف عام 2012، على الصعيد العالمي.[1] فالرسائل الإلكترونية الطفيلية تعتبر بالأحرى مسألة تتعلق بالقَبول من المحتوى. وغالبا ما تُعرف الرسائل الإلكترونية الطفيلية بأنها إرسال كميات كبيرة من الرسائل غير المرغوب فيها.[2] وغني عن البيان أن المشكلة التي تسببها الرسائل الإلكترونية الطفيلية تتعدى حد اسْتِيَاء مستخدمي الإنترنت،[3] نظرا لأن هذه الرسائل تستهلك المصادر مثل عرض النطاق الترددي، قدرة الخادم، والبنية التحتية للشبكات، علاوة على أن هذه الرسائل تشكل نقطة دخول لانتشار أي من

البريد الإلكتروني الطفيلي: مشروع القانون النموذجي للكوميسا

المادة 19– الدخول غير المصرح به لبرامج الحاسوب، البيانات الحاسوبية، بيانات المحتوى، بيانات الحركة

...

(ز) إرسال البريد الإلكتروني الطفيلي

أي شخص يرسل أي معلومات إلكترونية غير مرغوب فيها إلى شخص آخر بغرض التجارة أو التَعَامُل غير المشروع أو أي أنشطة أخرى غير قانونية، يعتبر مرتكبا لجريمة، معاقب عليها بغرامة [قيمتها]____ و/أو السجن لمدة____عاما، أو كليهما.

---

[1] Symantec Intelligence Report, June 2012; Kaspersky Lab Report, June 2012

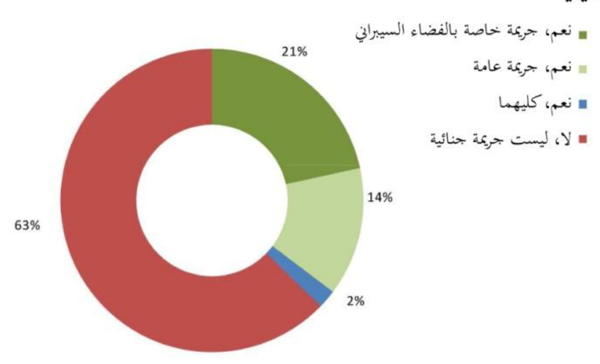
[2] For a working (rather than legal) definition, see http://www.spamhaus.org/consumer/definition/

[3] Sorkin, D., 2001. Technical and Legal Approaches to Unsolicited Electronic Mail. *University of San Francisco Law Review*, 35(2):325-384

البرمجيات الخبيثة وانتحال الصفة للحصول على كلمات سر الدخول، بالإضافة إلى المعلومات المالية. وبالتالي، وفي ضوء ما تقدم، فإن هذه الرسائل ترتبط بسلوك التدخل غير القانوني في البيانات الحاسوبية أو نظم الحاسوب، سواء بشكل مباشر أو غير مباشر، مما يهدد سلامة وتوافر البيانات والنظم.

وبالرغم من ذلك؛ تعتبر مواءمة الاتجاهات القانونية تجاه البريد الإلكتروني الطفيلي لم تكتمل بعد.[1] ويطرح اثنان من الصكوك (غير الملزمة) متعددة الأطراف المعنية بمكافحة الجريمة السيبرانية تجريم البريد الإلكتروني الطفيلي في المادة (19) من مشروع القانون النموذجي للسوق المشتركة لشرق وجنوب أفريقيا، والمادة (15) من النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/مجموعة الكاريبي/الاتحاد الكاريبي للاتصالات. هذا، وتتضمن الصكوك – غير الملزمة – متعددة الأطراف المعنية بمكافحة الجريمة السيبرانية أحكاما تتعلق بالبريد الإلكتروني الطفيلي، رغم أن ديباجة توجيه الاتحاد الأوروبي بشأن حماية البيانات تنص على أنه: "من الضروري حظر استعمال هويات مزورة أو عناوين ارْتِدادية غير حقيقية أو لحظة إرسال عدد من الرسائل غير المرغوب فيها لأغراض التسويق المباشر".[2] بالإضافة إلى ذلك؛ فإن الفقرة 3 من المادة 13 من نفس التوجيه تتطلب من الدول أن "تتخذ التدابير المناسبة لضمان أن "الرسائل غير المرغوب فيها لأغراض التسويق المباشر بغير مقابل وتعتبر غير مسموح بها بدون موافقة". ومع ذلك، فإن التوجيه لم يشترط صراحة إقْرار جريمة خاصة بموجب القوانين الداخلية للدول الأعضاء.

الشكل 4–20: تجريم إرسال أو التحكم بإرسال الرسائل الإلكترونية الطفيلية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 33. (رقم=51)

تشير الردود على الاستبيان الملحق بهذه الدراسة إلى أن حوالي ثلث الدول المجيبة فقط تعتبر إرسال أو السيطرة على إرسال بريد إلكتروني

البريد الإلكتروني الطفيلي: مثال وطني من دولة في جنوب آسيا

عقوبة التسبب بإتلاف حاسوب، نظام حاسوبي، إلخ.

أي شخص:

(ح) لأغراض الإعلان عن سلع أو خدمات يقوم أو يضطلع بإرسال بريد إلكتروني طفيلي، أو يرسل بريدا إلكترونيا غير مرغوب فيه بدون أي تصريح من المنشئ أو المشترك،....

(2) كل شخص يقوم بأي من الأفعال التي تخالف أيا من الأحكام الواردة في البند (1) يرتكب جريمة، ويعاقب طبقا للعقوبات الواردة في البند_____.

[1] De Hert, P., Fuster, G., Koops, B. J., 2006. Fighting cybercrime in the two Europes. The added value of the EU framework decision and the Council of Europe Convention. *International Review of Penal Law*, 77(3-4):503-524

[2] ديباجة توجيه الاتحاد الأوروبي بشأن حماية البيانات (43).

بشكل عشوائي جريمة جنائية، كما أنه من الواضح أن هذه الدول استخدمت كلّا من الجرائم العامة والجرائم الخاصة بالفضاء السيبراني. وقد تمخض عن استعراض المصدر الرئيسي للتشريعات المتاحة أن تسع دول فقط من 100 دولة تقريبا لديها أحكام جنائية خاصة -يمكن تحديدها- تتعلق بالبريد الإلكتروني الطفيلي. أما في ما يتعلق بمحل جريمة البريد الإلكتروني الطفيلي فإنه يختلف من "إرسال عدد ضخم من الرسائل غير المرغوب فيها" إلى تجريم تَحْرِيف "أصل الرسائل" أو "العناوين الرئيسية للرسالة". وعلى سبيل المثال في هذا الصدد، فإن إحدى دول الأمريكتين قد اعتمدت أحكاما جنائية تعاقب على التحريف في سطور موضوع الرسالة الإلكترونية. وفي بعض الدول، فإنه من المرجح أيضا وجود جزاءات إدارية لإرسال أو السيطرة على إرسال رسائل إلكترونية طفيلية.

وتتضمن الأفعال الرئيسية التي تعتبر محل تجريم البريد الإلكتروني الطفيلي "إرسال" رسائل طفيلية، أو إرسال عدة رسائل إلكترونية، أو الأفعال التي تَخدَع متلقي الرسالة، مثل "التلاعب" في معلومات موضوع الرسالة أو مصدرها. أما فيما يتعلق بالركن المعنوي، فإن مشروع القانون النموذجي للسوق المشتركة لشرق أفريقيا والجنوب الأفريقي يشترط أن يكون الفعل عمدا ومقترنا بنية ارتكاب أغراض غير مشروعة. أيضا تشترط النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/مجموعة الكاريبي/الاتحاد الكاريبي للاتصالات تجريم الأفعال المرتكبة بشكل متعمد، وإلى جانب ذلك، فإن الفعل المتعمد يعتبر مطلوبا أيضا من قبل تلك الأحكام الوطنية التي يمكن تحديدها وتحليلها.

وختاما، بينما لم يتصد أي صك دولي غير ملزم لمشكلة البريد الإلكتروني الطفيلي صراحة، إلا أن العناصر التهديدية التي تنتج عن البريد الإلكتروني الطفيلي مثل البرمجيات الخبيثة والتصيد الاحتيالي، قد تم تناولها من خلال الأحكام الواردة في الصكوك الدولية والإقليمية المعنية بحماية السرية، والنزاهة، وتوافر بيانات حاسوبية أو نظم حاسوب.

الاحتيال والتزوير المتعلق بالحاسوب

من المستقر أن المصلحة القانونية المحمية عند ارتكاب جرائم ضد السرية، والنزاهة، وتوافر بيانات حاسوبية أو نظم حاسوب تتمثل في سلامة المعلومات والبيانات الحاسوبية نفسها. على النّقِيضِ مِنْ ذلك، فإن الأحكام الجنائية بشأن استعمال الحواسيب في الاحتيال والتزوير تعمل على حماية

الاحتيال المرتبط بالحاسوب: اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية

المادة 8:

يعتمد كل طرف ما قد يلزم من تدابير تشريعية وغيرها بحسب الحاجة للنص على اعتبار الأفعال التالية، عندما ترتكب عن عمد أو دون وجه حق، جرائم بموجب قانونه الداخلي، وتتسبب في خسارة في ممتلكات لشخص لآخر، من خلال:

أ. أي إدخال بيانات حاسوبية أو تعديلها أو حذفها أو طمسها؛

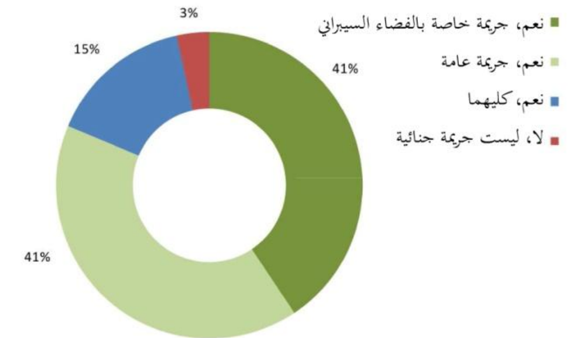
ب. أي تدخل في وظائف نظم أحد الحواسيب،

مع توافر نية احتيالية أو تدليسية لتحقيق مكاسب مالية بدون وجه حق لنفسه أو لشخص آخر.

المصالح المتمثلة في الممتلكات والأصول المالية والمستندات الموثقة.[1] وبالنظر إلى المستوى الدولي والإقليمي، فإن ثمانية صكوك تتضمن أحكاما بشأن تجريم استعمال الحاسوب في الاحتيال.[2] أما الأفعال التي تناولتها هذه الصكوك فإنها تتعلق بالتلاعب في البيانات الحاسوبية، أو التدخل غير القانوني في أحد أنظمة الحاسوب والذي يحقق مكاسب مالية للجاني أو لشخص آخر.

هذا، وتتضمن أيضا ستة صكوك أحكاما خاصة بشأن التزوير.[3] ومن الأفعال التي تناولتها الأحكام المعنية بالتزوير، تغيير البيانات الحاسوبية أو حذفها، أو نقلها، ووسائل التلاعب الأخرى في البيانات الحاسوبية، مما يؤدي إلى تزييف التاريخ، وذلك بنية استعمال البيانات أو التصرف فيها كما لو كانت بيانات أصلية.

الشكل 4-21: تجريم استعمال الحواسيب في الاحتيال والتزوير



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 30. (رقم=59)

ومع ذلك، وعلى المستوى الوطني، يختلف الوضع إلى حد كبير فيما يتعلق بوجود أحكام سيبرانية خاصة تجرم الاحتيال والتزوير. وفي هذا الصدد، أشارت الدول المجيبة على الاستبيان المرافق لهذه الدراسة إلى أن التشريعات العامة الموجودة قد تناولت استعمال الحاسوب في الاحتيال والتزوير (أكثر من 40 في المائة)، وتقريبا نفس النسبة المذكورة أفادت بوجود جرائم خاصة بالفضاء السيبراني، في حين أن نسبة 12 في المائة فقط تستعمل كلا من المنهجين.[4]

---

[1] Sieber, U., 1998. *Legal Aspects of Computer-Related Crime in the Information Society COMCRIME-Study.* Available at: www.edc.uoc.gr/~panas/PATRA/sieber.pdf.

[2] مشروع اتفاقية الاتحاد الأفريقي المادة 26/ج، 41/ج، مشروع القانون النموذجي لدول الكوميسا المادة 24، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المادة 8، المشروع التوجيهي للجماعات الاقتصادية لدول غرب أفريقيا المادة 10 قرار الاتحاد الأوروبي بشأن الاحتيال والتزوير المادة رقم 2، النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/مجموعة الكاريبي/الاتحاد الكاريبي للاتصالات المادة 12، الاتفاقية العربية بشأن مكافحة جرائم المعلومات المادة 10، 11. القانون النموذجي العربي لمواجهة الجريمة السيبرانية المواد 10-12.

[3] مشروع اتفاقية الاتحاد الأفريقي المادة 24/ج، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المادة 7، مشروع القانون النموذجي لدول الكوميسا المادة 23، النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/موجوعة الكاريبي/الاتحاد الكاريبي للاتصالات المادة 11، القانون النموذجي العربي لمواجهة الجريمة السيبرانية المادة 4، المشروع التوجيهي للجماعات الاقتصادية لدول غرب أفريقيا المادة 8.

[4] الاستبيان الخاص بالدراسة، السؤال رقم 30

ينبع هذا التنوع جزئيا من الاختلاف بين النظم القانونية الوطنية في سياق إمكانية تطبيق الجرائم "التقليدية" في بيئة الإنترنت. فعلى سبيل المثال؛ جرائم الاحتيال التقليدية غالبا ما تتطلب الخداع المباشر "لأحد الأشخاص"، وربما تمرّ بتحديات في توسيع نطاقها للأفعال المرتكبة خلال التلاعب بإحدى البيانات الحاسوبية أو نظم الحاسوب.[1] وعلى نحو مماثل؛ فإن جرائم التزوير التقليدية غالبا ما تشترط تغيرا في "التمثيل المرئي"، وفقا للنهج القانوني الوطني، بيد أن ذلك يعد متطلبا قد لا يكفي عند تغيير بيانات غير ملموسة تحتويها أجهزة إلكترونية.[2]

استعمال الحاسوب في أعمال التزوير: مشروع اتفاقية الاتحاد الأفريقي

المادة 3 – 8

يجب على كل دولة عضو في الاتحاد الأفريقي اتخاذ التدابير التشريعية لاعتبار حقيقة إنتاج أو تصنيع مجموعة واسعة من البيانات الرقمية من خلال مدخل احتيالي أو حذف أو طمس بيانات محوسبة مَنْقُولة أو معالجة أو إرسالها من قبل أحد الأنظمة الحاسوبية، والتي تؤدي إلى وجود بيانات وهمية بهدف اتخاذ البيانات المذكورة بعين الاعتبار أو استعمالها في أغراض غير قانونية كما لو كانت هذه البيانات بمثابة بيانات أصلية، بمثابة جنحة جزائية.

ومن أجل التعامل مع هذه التحديات القانونية، غالبا ما تركز الأحكام الوطنية المعنية بالاحتيال الخاص بالفضاء السيبراني على التلاعب بالبيانات الحاسوبية أو نظم الحاسوب بنية مضللة أو احتيالية، أو بالأحرى عناصر خداع أي شخص. وفي بعض الدول، تجرم أحكام استعمال الحاسوب في عمليات الاحتيال أيضا استخدام البيانات بدون تصريح، إلى جانب ذلك استعمال بيانات وهمية (أنظر المثال الوارد أدناه بشأن إحدى دول جنوب آسيا). وهذا يمكن أن يؤدي – على سبيل المثال – إلى تطبيقات واسعة للأحكام المعنية باستعمال الحاسوب في الاحتيال لكل الحالات التي يستخدم فيها الحاسوب في الإثراء غير المشروع.[3] وتجدر الإشارة؛ إلى أن عددا من الدول تواصل تعديل القوانين الوطنية لإدراج

ضَمّ أحكام الاحتيال والتزوير المتصلين بالحواسيب:
مثال وطني من دولة في جنوبي أفريقيا

(1) يعتبر مرتكبا لجريمة أي شخص يقوم بأداء أي من الأفعال المنصوص عليها بموجب هذا الجزء، لأغراض الحصول على أي مزية غير مشروعة عن طريق التسبب في تزوير بيانات قد يتم انتاجها بقصد اعتبار هذه البيانات كما لو كانت أصلية أو التصرف بناء على أنها أصلية، يعاقب في حالة الإدانة بغرامة _____ أو بالسجن _____، أو العقوبتين معا.

(2) يعتبر مرتكبا لجريمة أي شخص يتسبب بشكل احتيالي في إلحاق خسائر بممتلكات تخص شخصا آخر بقصد الحصول على أي منفعة لنفسة أو لشخص آخر عبر –

(أ) أي إدخال بيانات أو تعديلها أو حذفها أو طمسها؛ أو

(ب). أي تدخل في الأداء الوظيفي للحاسوب أو نظم الحاسوب،

ويعاقب في حالة الإدانة بغرامة _____ أو بالسجن _____، أو العقوبتين معا.

[1] Sieber, U., 2008. Mastering complexity in the global cyberspace : The harmonization of computer-related criminal law. In : Delmas-Marty, M., Pieth, M. and Sieber, U., (eds.) *Les chemins tie l'Harmonisation Penale/Harmonising Criminal Law. Collection tie L'UMR tie Droit Compare tie Paris.* Vol. 15. Paris: Société de législation comparé

[2] المرجع السابق.

[3] See Sieber, U., 1985. *Informationstechnologie und Strafrechtsreform.* Cologne: Carl Heymanns Verlag, p.39.

استعمال الحاسوب في الاحتيال ضمن الجرائم الخاصة بالفضاء السيبراني. ومن الملاحظ، على سبيل المثال، أن إحدى دول أوروبا الشرقية قامت مؤخرا باعتماد مادة جديدة في قانونها الجنائي تتعلق بالاحتيال المتصل بالحاسوب، وذلك بعد أكثر من عشر سنوات من الملاحقات القضائية لحالات الاحتيالي الحاسوبي بموجب مزج الأحكام العامة المعنية بالاحتيال بالأحكام المعنية بالنفاذ غير المشروع، وبالرغم من أنها قد دعمت هذا النهج في وقت سابق، إلا أن عملية الإصلاح التي قد أطلقتها المحكمة العليا بهدف ضمان وجود ملاحقة قضائية أكثر كفاءة للمشتبه بهم، بالإضافة إلى إزالة أي التباس قانوني متبقي بشأن تطبيق أحكام التزوير التقليدية.

كما تطبق بعض الدول أيضا أحكاما تتعلق بالسرقة في حالات الاحتيال الحاسوبي على اعتبار أن البيانات الحاسوبية تندرج تحت تعريفات "السلع"، و"الأشياء"، وقد أخذت بعض الدول في أوروبا الغربية وأوروبا الشمالية، وأمريكا الشمالية بهذا النهج. ومن ناحية أخرى، فإن العديد من الدول تزيد عن ذلك، حيث لديها أحكام تتعلق "بالسرقة التقنية" أو السرقة التي تتضمن استخدام نظم الحاسوب لارتكاب الجريمة (أُنظر المثال الوراد أدناه بشأن إحدى دول غرب آسيا).

وعادة ما تشترط الأحكام الوطنية المعنية بالتزوير المتصل بالحاسوب عنصرين أساسيين: (1) تغيير البيانات الحاسوبية أو التلاعب فيها، (2) توافر نية محدد تتمثل في استعمال البيانات كما لو كانت بيانات حَقِيقِيّة. وكبديل لذلك، يمكن للدول أن توسع من نطاق تعيين محل جريمة التزوير التقليدية. فعلى سبيل المثال؛ قامت إحدى الدول الأوروبية بالتصدي للتزوير المتصل بالحاسوب من خلال توسيع نطاق تعريف ماهية "الوثيقة" لتدرج ضمن تعريفات البيانات الحاسوبية. بيد أن الدول الأخرى تطبق أحكاما عامة على استخدام الحاسوب في أعمال الحاسوب دون تعديل التشريعات، بحيث في حالة تفسير الأحكام المتعلقة بجريمة التزوير التقليدية فإن ذلك التفسير يشمل الوثائق الرقمية والتوقيعات الرقمية، علاوة على البيانات الرقمية.

استعمال الحاسوب في أعمال التزوير: مثال وطني من دولة في جنوب أوروبا

المادة ـــ التزوير الحاسوبي

(1) أي شخص أيا ما كان يقوم بدون تصريح بتطوير أو تركيب أو تغيير أو حذف أو يجعل بيانات الحاسوب أو برامجه غير صالحة للاستعمال والتي تعتبر ذات أهمية للعلاقات القانونية بغية استخدامها باعتبارها علاقات صحيحة، أو أي شخص يستعمل هذه البيانات أو البرامج، يعاقب بغرامة ـــــ وبالسجن لمدة لا تتجاوز ـــــ.

(2) في حالة إذا كان محل ارتكاب الجريمة الجنائية المشار إليها في المادة 1 بيانات حاسوبية أو برامج حاسوبية تخص إحدى الهيئات الحكومية أو مؤسسة عامة أو شركة خاصة ذات مصلحة عمومية، أو إذا كان الضرر المتسبب كبيرا، يعاقب الجاني في هذه الحالة بالسجن لمدة ـــــ.

الجرائم المتصلة بالهوية

الجرائم المتصلة بالهوية

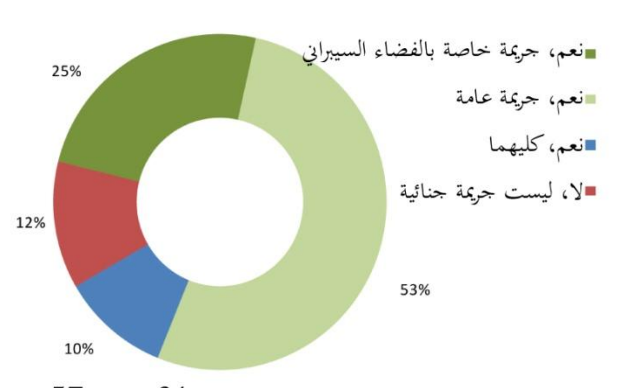
نصوص تشريعية نموذجية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات

المادة 14

أي شخص يقوم، عمدًا وبدون عذر أو مبرر قانوني، أو يتَجَاوُز العذر والمبرر القانوني، باستعمال نظام حاسوبي (في أي مرحلة من مراحل الجريمة) بشكل عمدي بإرسال أو حيازة أو استعمال، بدون عذر أو مبرر قانوني، هوية شخص آخر بنية ارتكاب أو لمساعدة أو للتحريض أو للعمل بموجبها في أي نشاط غير مشروع يشكل جريمة، فإنه والحالة يعتبر مرتكبا لجريمة، معاقب عليها (في حالة الإدانة) بالسجن لمدة لا تتجاوز [....] أو بغرامة لا تتجاوز [...]، أو العقوبتين معا.

لقد شكلت الموصولية العالمية والمعالجة الآلية للبيانات بالإضافة إلى تطور المعاملات التجارية التي لا تتم وجها لوجه، مزيدا من فرص سرقة المعلومات ذات الصلة بالهوية والبيانات الشخصية ومن خلال نظم الحاسوب.[1] وتتجسد أهداف هذه الجريمة في كل من المعلومات "التقليدية" بشأن الهوية، إلى جانب الأنواع الجديدة من المعلومات التعريفية، ومنها أرقام بطاقات الائتمان، ومعلومات بشأن الحسابات المصرفية، وأرقام جوازات السفر ورخص القيادة، وحسابات الإنترنت، وكلمات المرور، وعناوين برتوكولات الإنترنت. ومن الجائز أن تكون محل العديد من الأعمال التي تشكل جرائم سرقة الهوية، بما في ذلك الحصول على معلومات تتعلق بالهوية واستخدامها. فعلى سبيل المثال، يمكن التحصل على البيانات عن طريق النفاذ غير المشروع للنظام الحاسوبي، وذلك من خلال استعمال برمجيات ضارة أو استخدام التصيد الاحتيالي (وهو في حد ذاته يشكل جريمة تزوير تتصل بالحاسوب) أو عن طريق الاستحواذ غير المشروع على البيانات الحاسوبية، مثل الأشخاص "المطلعين" على أمور الشركات.

الشكل 4-22: تجريم استعمال الحواسيب في جرائم الهوية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 31. (رقم=57)

وتوجد مجموعة من الاتجاهات تتعلق بتناول القانون الجنائي للأفعال المتمثلة في الحصول على بيانات الهوية واستعمالها وإرسالها وذلك للأغراض الجنائية. ومن الملاحظ أن النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات (المادة 14) تعتبر الصك الوحيد (غير ملزم) على المستوى الدولي والإقليمي الذي تُعنى

[1] UNODC, 2011. *Handbook on Identity-related Crime.* Available at: http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

أحكامه بسرقة الهوية. ويتناول هذا الحكم الأفعال المرتكبة باستعمال أحد أجهزة الحاسوب في أي مرحلة من مراحل الجريمة والتي تتمثل في قيام الجاني بشكل متعمد بإرسال أو حيازة أو استعمال، بدون عذر أو مبرر قانوني، هوية شخص آخر "بنية ارتكاب أو للمساعدة أو للتحريض أو للعمل بموجبها في أي نشاط غير مشروع يشكل جريمة.

الجرائم المتعلقة بالهوية: مثال وطني من دولة في الكاريبي

سرقة الهوية. المادة ---

أي شخص يستخدم حاسوبا أو يجعل الحاسوب عن علم أن يؤدي أي وظيفة بهدف الوصول لعناصر تأمين أي برنامج أو بيانات موجودة في هذا الحاسوب أو في أي حاسوب آخر بهدف انتحال شخصية صفة شخص آخر أو سرقة أو انتحال هوياتهم، يعتبر مرتكبا لجريمة ويعاقب في حالة إدانته بغرامة قدرها _____ وبالحبس لمدة _____.

وعلى المستوى الوطني، تظهر ردود الدول على الاستبيان المرافق لهذه الدراسة بأن نسبة قليلة نسبيّا من الدول– 25 في المائة – تفيد بوجود أحكام خاصة بالفضاء السيبراني تتعلق بالجرائم ذات الصلة بالهوية، وعلى النقيض من ذلك، أفاد ما يزيد عن نسبة 50 في المائة من الدول بأنها تستعمل الأحكام العامة. بيد أن نسبة 10 في المائة من الدول قد أفادت بأن الأفعال ذات الصلة بالهوية لا تشكل جريمة جنائية.

وباستقراء تحليل المصدر الرئيسي للتشريعات، يتضح أن–لجرائم الهوية الخاصة في الفضاء السيبراني –محل جريمة سرقة الهوية يعتبر عادة بمثابة "بيانات" (أو "بيانات شخصية") أو المعلومات التعريفية. ومن الملاحظ أن في حالة وجود أحكام، فإنها لا تتناول دائما كل الأفعال التي يمكن أن تشكل على الأرجح أركان جريمة سرقة الهوية. فعلى سبيل المثال؛ لا تدرج بعض الدول الأفعال المعنية "بإرسال" البيانات الشخصية ولكن بالأحرى تقصر التجريم على الأفعال التي "تُستخدم فيها" وسائط الهوية و"الحصول" عليها. بيد أن الأحكام الأخرى تقتصر فقط على مسألة "الحصول" على بيانات الهوية، أو تستبعد كلا من الحصول والاستخدام على الإطلاق من نطاق الأفعال المشكلة لجرائم الهوية (أُنظر المثال المدرج الخاص بإحدى دول منطقة الكاريبي). وباستجلاء الواقع، فإن بعض القوانين الوطنية ذهبت أبعد من ذلك، حيث تجرم تَألِيف بيانات شخصية كاذبة. وبإيجاز؛ فإن استعراض المصدر الرئيسي للتشريعات يشير إلى الانخفاض النسبي لعدد الدول التي لديها أحكام تتعلق بجرائم الهوية في الفضاء السيبراني، إلى جانب الدول التي قامت باعتماد مثل هذه الأحكام، يوجد تباين كبير في النهج المتبعة. وغني عن البيان، إذا تناولت القوانين العامة الجرائم ذات الصلة بالهوية، فإن ذلك يمكن تحقيقه من خلال عدد من الأحكام المختلفة، بما فيها الأحكام المعنية بالنفاذ غير المشروع، والتدخل غير القانوني في البيانات، وأدوات إساءة استعمال الحاسوب، والاحتيال والتزوير المتصلين بالحاسوب.

جرائم استغلال الأطفال في المواد الإباحية

استغلال الطفل في المواد الإباحية: البروتوكول الاختياري لاتفاقية حقوق الطفل

المادة 3

(1) تكفل كل دولة طرف أن تغطي، كحد أدنى، الأفعال والأنشطة التالية تغطية كاملة بموجب قانونها الجنائي أو قانون العقوبات فيها سواء أكانت هذه الجرائم ترتكب محليّا أو دوليّا أو كانت ترتكب على أساس فردي أو منظم: ...
(ج) وإنتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالطفل على النحو المعرَّف في المادة 2. ...
(3) تتخذ كل دولة طرف التدابير اللازمة التي تجعل هذه الجرائم موجبة للعقوبات المناسبة والتي تضع في الاعتبار خطورة طابعها.

تُرسل تقريبا كل الصور المتضمنة مواد إباحية تتعلق بالأطفال إلكترونيا من خلال التبادلات الثنائية أو متعددة الأطراف.[1] وتتضمن المصالح المحمية من خلال تجريم استغلال الأطفال في المواد الإباحية، حماية القصر من الاعتداء وتعطيل أسواق الصور المتضمنة مواد إباحية تتعلق بالأطفال، والتي من شأنها أن تدفع الجناة إلى السعي نحو إنتاج وتوريد المزيد من الصور.[2] هذا ويوجد على المستوى الدولي والإقليمي، تسعة صكوك محددة تتضمن أحكاما تجرم الأفعال ذات الصلة باستغلال الأطفال في المواد الإباحية.[3] بالرغم من أن الأطر الدولية تظهر العديد من أوجه التشابه فيما يتعلق بتجريم استغلال الأطفال في المواد الإباحية، إلا أنه توجد اختلافات أيضا تتعلق بمحل الجريمة والفئة العمرية للأطفال، وماهية الأفعال التي تتناولها.

أشار ما يزيد عن نسبة 80 في المائة من الدول المجيبة – على المستوى الوطني – على الاستبيان الملحق بهذه الدراسة إلى أن استغلال الطفل في المواد الإباحية يعتبر جريمة جنائية، كما أفادت غالبية الدول بأن هذه الأفعال تعتبر مجرمة من خلال إحدى الجرائم العامة. الأفعال التي تنطوي على استغلال الطفل في المواد الإباحية يمكن ارتكابها عبر مجموعة واسعة من الوسائط الإعلامية، ومنها الصور "دون الاتصال بالإنترنت"، ويعتبر النهج العام "للتكنولوجيا والحياد الإعلامي" بمثابة أحد أساليب جرائم الحاسوب الخاصة التي تأخذ بها العديد من الدول. وفي هذا الصدد، أوضح عدد من الدول المجيبة على الاستبيان الملحق بهذه الدراسة أن استغلال الطفل في المواد الإباحية مُجرم في سياق المواد الإباحية بشكل عام. وهذا ما عززه تحليل المصدر الرئيسي للتشريعات، حيث وجد أن هناك دولتين لديهما أحكام عامة بشأن المواد الإباحية، بما في ذلك استغلال الطفل في المواد الإباحية. أما فيما

---

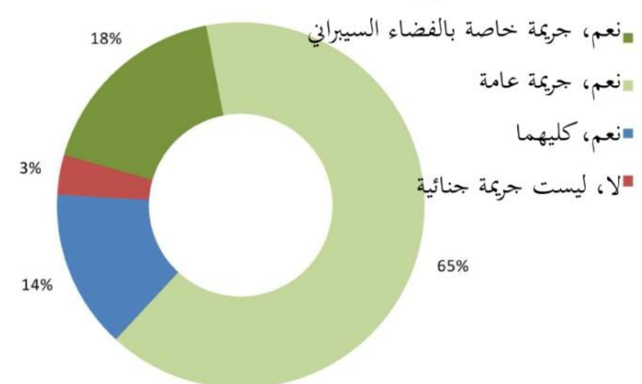
[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة 2010، عولمة الجريمة. تقييم تهديد الجريمة المنظمة عبر الوطنية، الفصل العاشر. متاح على الرابط التالي: http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf, p.212.

[2] See Hamilton, M., 2011-2012. The child pornography crusade and its net-widening effect. *Cardozo Law Rev,* 33(4):1679-1732.

[3] مشروع اتفاقية الاتحاد الأفريقي، المواد 29/ج، 32/ج، القانون النموذجي لدول اتحاد الكومنولث المادة 10، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المادة9، اتفاقية دول الاتحاد الأوروبي بشأن حماية الطفل المادة 20، المشروع التوجيهي للجماعة الاقتصادية لدول غرب إفريقيا المادة 14، و17، التوجيه الأوروبي بشأن استغال الطفل المادة 5، النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات السلكة واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات المادة 13، الاتفاقية العربية بشأن مكافحة جرائم المعلومات المادة 12، الأمم المتحدة اتفاقية حقوق الطفل–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن اشتراك الأطفال في النزعات المسلحة– البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء والمواد الإباحية المادة 3

يتعلق بالدول التي ليس لديها أحكام خاصة بشأن استغلال الطفل في المواد الإباحية، فإنه من الممكن الملاحقة القضائية لهذه المواد من خلال استخدام قوانين ذات نطاق أوسع تستوعب تجريم المواد المتعلقة بالفُحْش أو المواد المسيئة. وأخيرا، يظهر تحليل التشريعات، من تلك الدول التي لديها أحكام خاصة باستغلال الطفل في المواد الإباحية، العديد من أوجه التشابه، فضلا عن وجود اختلافات بين *محل الجريمة* و*الركن المادي* المكون لها.

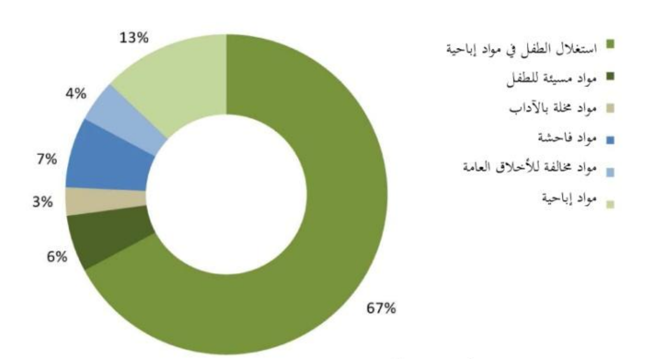
الشكل 4–23: تجريم إنتاج، توزيع، أو حيازة مواد إباحية تستغل الطفل ذات صلة بالحاسوب



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 36. (رقم=57)

محل الجريمة – تستخدم مُعْظَم الصكوك الدولية والإقليمية مصطلح "استغلال الطفل في المواد الإباحية" لتحديد ماهية محل الجريمة. بيد أن الاتفاقية العربية بشأن مكافحة جرائم المعلومات تستخدم مصطلح "المواد الإباحية المتعلقة بتصوير أحد الأطفال". ويبين الشكل 4–24 تباينا في المصطلح المستخدم على المستوى الوطني. وتستخدم تقريبا نسبة 70 في المائة من 70 دولة من التي خضعت أحكامها للاستعراض، مصطلح "استغلال الطفل في المواد الإباحية"، بيد أن ما يزيد عن نسبة 10 في المائة تستخدم مصطلح " المواد الإباحية المتعلقة بتصوير أحد الأطفال". أما المصطلحات الأخرى المغايرة لما ذكر أعلاه، فتتمثل في "مواد فاحشة تتعلق بتصوير أحد الأطفال"، "مواد إساءة التعامل مع الطفل"، "المواد التي تنطوي على أحد الأطفال بما يناهض الأخلاق العامة"، و"تصوير أحد الأطفال بشكل داعِر". ومن الملاحظ في هذا الصدد؛ هو عدم قدرة النصوص التشريعية وحدها وبمنأى عن تفسير السلطات

الشكل 4–24: المصطلحات المستخدمة في الأحكام ذات الصلة باستغلال الطفل في المواد الإباحية حاسوبيا



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=70)

القضائية الوطنية للأحكام على تقييم ما إذا كانت تترجم الاختلافات في المصطلحات المستخدمة إلى اختلافات عملية بنفس الطبيعة للمواد المجرمة.

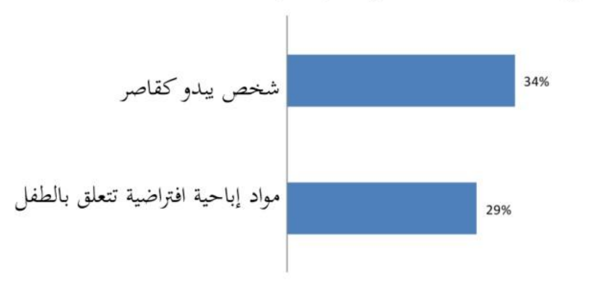
ومع ذلك، فإن التشريعات يمكنها أن تحدد نطاق الوسائط المدرجة ضمن الجريمة، فعلى سبيل المثال، تشير بعض من الصكوك الدولية والإقليمية إلى "المواد البصرية" و"النصوص" التي تبَيّن كيفية استغلال الطفل في المواد الإباحية. بيد أن تحديد الوسائط المدرجة بهذه الطريقة قد يشكل، مع ذلك، خطرا يتمثل في استبعاد المواد السمعية من نطاق الوسائط. ولذلك، هناك عدد من الصكوك (منها النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، والتوجيه الأوروبي بشأن استغلال الأطفال) تشير إلى استخدام "أي عرض من العروض باستخدام أي وسيلة كانت". إلا أنه من ناحية أخرى، يميل كل من اتفاق مجلس أوروبا بشأن الجريمة السيبرانية والقانون النموذجي لدول اتحاد الكومنولث إلى استعمال "التفسير البصري" لاستغلال الطفل في المواد الإباحية، وبالتالي تُستبعد المواد السمعية. ويظهر استعراض التشريعات على المستوى الوطني أن حوالي ثلث الدول التي خضعت للتحليل تقصر محل التجريم على المواد المرئية أو العروض البصرية. أما فيما يتعلق بالدول الأخرى الباقية، فإنها تتبنى النصوص والملفات الصوتية (بشكل أقل في أغلب الأوقات) أو تشير إلى أي عرض من العروض أيا كان.[1]

استغلال الطفل في المواد الإباحية: مثال وطني من دولة في أوروبا الغربية

يعاقب بالسجن لمدة لا تزيد عن ____ عاما أو بغرامة ____ أي شخص يقوم بنشر أو عرض أو يعرض علنا أو يصنع أو يستورد أو يرسل أو يصدر أو يكتسب، أو يحوز إحدى الصور أو يضع على أحد حوامل البيانات صورة – لفعل جنسي يشترك أو يظهر فيه شخص لم يبلغ سن الثامنة عشر، أو من يتمكن من كسب الدخول إلى مثل هذه الصورة من خلال جهاز أو نظام محوسب أو من خلال خدمة اتصالات.

أما الاختلاف الثاني بين الاتجاهات القانونية فيتعلق بإنتاج المواد التي لا تنطوي على أطفال، ويتضمن ذلك، استخدام الحاسوب في عروض المحاكاة أو الصور الواقعية لطفل غير موجود أو مواد تنطوي على أشخاص بلغوا سن الرشد (لأغراض حظر انتاج المواد الإباحية) ولكن يبدو أنهم قُصّر. وتتضمن أغلب الصكوك الدولية أو

الشكل 4–25: تجريم استعمال الحاسوب في إنتاج أو توزيع أو حيازة مواد تحاكي استغلال الأطفال في المواد الإباحية

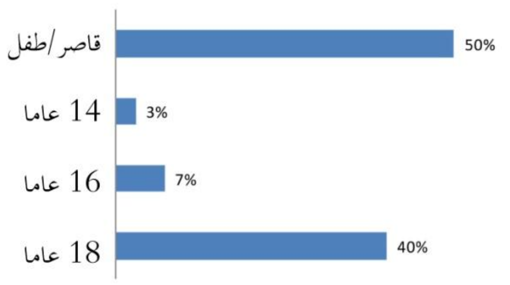


المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=70)

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استعراض التشريعات.

الإقليمية هذا النمط من المواد التي تدخل في نطاق التجريم،[1] بالرغم من أن بعض الصكوك تجيز للدول عدم تجريم الصور الحقيقية.[2] بيد أنه على المستوى الوطني، لا تتبع جميع الدول هذا النهج. وأما ما يتعلق بالنتائج المستخلصة من الدول التي خضعت تشريعاتها للاستعراض، فإن نسبة 34 في المائة من الدول تتناول الصور الحقيقية للراشدين الذين "يبدون كالقُصّر"، أو الصور التي "تبدو أنها تنطوي على قُصّر"، أو الصور التي تعتبر "صور حقيقية لقُصّر"، فيما تنص نسبة 29 في المائة فقط من الدول التي خضعت تشريعاتها للتحليل على تجريم المواد الإباحية "الصُوْرِيّة" أو الافتراضية" المتعلقة بالطفل.

الشكل 4-26: مواصفات الفئة العمرية للضحية في الأحكام المعنية باستخدام الحاسوب في استغلال الأطفال في المواد الإباحية



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=70)

أما الاختلاف الثالث فيتمثل في الفئة العمرية للطفل المستخدم في التمثيل الإباحي. فقد عنيت المادة الأولى من اتفاقية الأمم المتحدة لحقوق الطفل بتحديد الطفل بأنه كل إنسان لم يتجاوز الثامنة عشرة، بيد أن المادة من ناحية أخرى أبدت تحفظا تمثل في "قبل ذلك" بموجب القانون المنطبق على الطفل "ما لم يبلغ سن الرشد قبل ذلك".[3] وبينما تعتبر الدول الأطراف وفقا للاتفاقية غير مقيدة من حيث المبدأ بحد عمري لأقل من 18 عاما في التعريفات المعنية باستغلال الطفل في المواد الإباحية، إلا أن لجنة الأمم المتحدة لحقوق الطفل قد أوصت في عدة مناسبات بأن التعريفات يتعين أن تتناول كل الأطفال دون سن الثامنة عشر.[4] وفي هذا الصدد، تشير صكوك أخرى إلى حدود عمرية مختلفة. فعلى سبيل المثال؛ تحدد اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية بأن مصطلح "قاصر" يمتد ليشمل كل الأشخاص دون سن 18 عاما، كما تجيز الاتفاقية للدول الأطراف أن تضع حدّا عمريّا أقل "بحيث لا يقل عن 16 عاما". إلى جانب ذلك، فإن

---

[1] تم تناول ذلك بشكل صريح في: مشروع اتفاقية الاتحاد الأفريقي، المواد 1/ج، القانون النموذجي لدول اتحاد الكومنولث المادة 10، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية المادة9، اتفاقية دول الاتحاد الأوروبي بشأن حماية الطفل المادة 20، المشروع التوجيهي للجماعة الاقتصادية لدول غرب إفريقيا المادة 1، التوجيه الأوروبي بشأن استغال الطفل المادة2/ج، النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات السلكة واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات المادة 13، الاتفاقية العربية بشأن مكافحة جرائم المعلومات المادة 7/3، الأمم المتحدة اتفاقية حقوق الطفل–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن اشتراك الأطفال في النزعات المسلحة–البرتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء والمواد الإباحية المادة 2/ج

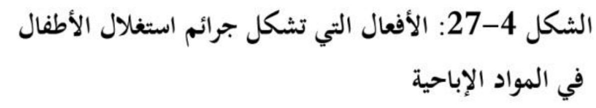
[2] اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، التوجيه الأوروبي بشأن حماية الطفل، متى استخدمت المادة لأغراض انتاجها ولا تشكل خطر من نشرها.

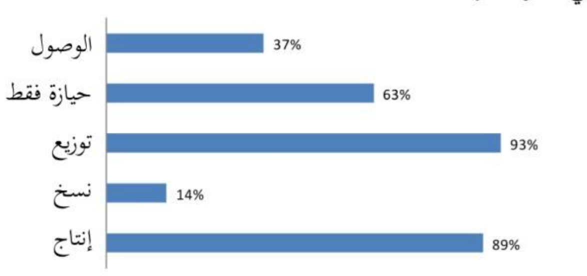
[3] اتفاقية الأمم المتحدة لحقوق الطفل، المادة (1)

[4] See, for example, CRC/C/OPSC/MNE/CO/1 (2010); CRC/C/OPSA/NOR/CO/1 (2005); CRC/C/OPSC/YEM/CO/1 (2009); and CRC/C/CUB/CO/2/ (2011).

الصكوك الأخرى، مثل الاتفاقية العربية بشأن مكافحة جرائم المعلومات أو القانون النموذجي لدول اتحاد الكومنولث، تستخدم مصطلح "الطفل" أو "القاصر" دون تحديد فئة عمرية.

على المستوى الوطني، يعتبر تحديد الفئة العمرية، التي يمكن معها تطبيق الأحكام المعنية باستغلال الأطفال في المواد الإباحية ليس واضحا، حيث إن العديد من الدول تشير إلى مصطلح "قاصر" أو "طفل" بدون تحديد فئة عمرية في المادة القانونية نفسها. وبالأحرى فإنه يمكن العثور على الفئات العمرية ذات الصلة في الأجزاء الأخرى من التشريعات الوطنية، لما فيها حماية الطفل أو التشريعات المعنية بحقوق الطفل. هذا، ويظهر الشكل 4-26 أنه في ضوء تحليل العديد من أحكام القانون الجنائي المتاحة، فإنه من غير الممكن تحديد الفئة العمرية ذات الصلة بشكل يسير (بدون تحليل مفصل للأجزاء الأخرى للقانون الوطني). وتجدر الإشارة هنا، إذا كان من الجائز تحديد الفئة العمرية من القانون الجنائي الوطني، فإن السواد الأعظم من الأحكام يشير إلى فئة الـ 18 عاما. وأخيرا، فإن القوانين الجنائية في عدد قليل من الدول تضمنت فئات عمرية محددة بـ 16 عاما أو 14 عاما، وذلك لأغراض تحديد ماهية المواد الإباحية ذات الصلة بالطفل. وفي هذا الصدد، فقد أعربت لجنة الأمم المتحدة لحقوق الطفل عن قلقها البالغ إزاء تحديد استخدام الفئة العمرية بـ 14 عاما.[1]


الشكل 4–27: الأفعال التي تشكل جرائم استغلال الأطفال في المواد الإباحية



المصدر: مراجعة تشريعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. (رقم=70)

الأفعال المشمولة – تشترط أغلبية الصكوك الدولية والإقليمية تجريم مجموعة واسعة من الأفعال المرتبطة باستغلال الطفل في المواد الإباحية، ومن هذه الأفعال؛ "إنتاج" و"عرض"، و"إتاحة"، و"توزيع"، و"إرسال"، و"حيازة". وتجرم بعض الصكوك أيضا معرفة "التمكن من الوصول" إلى المواد الإباحية المتعلقة بالطفل.[2] بيد أن القوانين الوطنية تظهر بعضا من التنوع فيما يتعلق بتلك الأفعال المدرجة ضمن أحكامها. وبالنظر إلى الشكل 4-27، يتضح أن نسبة 90 في المائة من الأحكام التشريعية الوطنية التي خضعت للاستعراض تجرم عموما الأفعال المتعلقة "بإنتاج" و"توزيع" مواد إباحية متعلقة بالطفل. كما أن ما يزيد عن نسبة 60 في المائة من الدول التي تم استعراض تشريعاتها تُجرم الأفعال المتعلقة "بالحيازة" مع نسبة 40 في المائة تتضمن أحكاما بشأن "الحصول على"

---

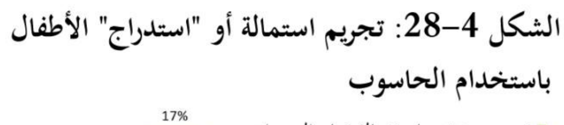
[1] أنظر على سبيل المثال؛ .CRC/C/OPSC/EST/CO/1 (2010) and CRC/C/OPSC/AUT/CO/1 (2008)
وترى اللجنة أيضا أن استعمال ظروف الجريمة مثل "نية النشر" و"وفي حالة عدم موافقة القاصر" لجرائم استغلال الطفل في المواد الإباحية المنطوية على أطفال تتراوح أعمارهم ما بين 14 و18 عاما تعتبر مخالفة للبروتوكول الاختياري لاتفاقية حقوق الطفل.

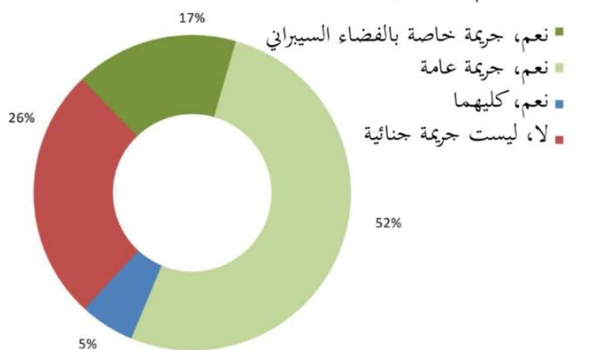
[2] مشروع اتفاقية الاتحاد الأفريقي، اتفاقية مجلس أوروبا المعنية بحماية الكفل، التوجيه الأوروبي بشأن استغلال الطفل، النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات السلكة واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات

مواد إباحية تتعلق بالطفل. وختاما لما ذكر، فإن في بعض الدول، تعتبر إمكانية امْتِداد تطبيق الأحكام المعنية "بالحيازة" على حالة المشَاهَدَة عبر الإنترنت أو الصور المتحركة لا تزال غير واضحة. بيد أن عددا من الدول الأوروبية تدرج أيضا مشاهدة المواد الإباحية المتعلقة بالأطفال عبر الإنترنت داخل نطاق الحيازة، وعلة ذلك تتمثل في حقيقة مفادها أن مشاهدة الصور تتضمن بالضرورة نسخ الصورة في ذاكرة الحاسوب و/أو ملفات ذاكرة التخزين المؤقت عبر الإنترنت. أما فيما يتعلق بالدول الأخرى، فقد قامت بوضع حلول، مثل اشتراط "*الأنشطة الاعتيادية*" من جانب الجاني.

استمالة الأطفال أو "استدراجهم" المتعلق بالحاسوب

تنظر القوانين الجنائية إلى "استدراج" الأطفال عبر الإنترنت باعتباره أحد أشكال تجريم الأفعال التحضيرية للاعتداء على الأطفال "دون الاتصال بالإنترنت".[1] وفي هذا الصدد، طالب صكان من المنطقة الأوروبية – اتفاقية مجلس أوروبا بشأن حماية الطفل (المادة 23) والتوجيه الخاص بالاتحاد الأوروبي بشأن استغلال الطفل (المادة 6) – بتجريم هذه الأفعال. وتتضمن العناصر الرئيسية للجريمة؛ عرضا متعمدا من قبل أحد الأشخاص الراشدين، من خلال وسائل تكنولوجيا المعلومات والاتصالات، للقاء أحد الأطفال "لأغراض" ارتكاب إحدى الجرائم. ومن أجل اكتمال الجريمة، فإن كلا من الصكين المذكورين اشترط أيضا "أفعال مادية" تقود إلى هذا اللقاء من قبل الجاني.


الشكل 4-28: تجريم استمالة أو "استدراج" الأطفال باستخدام الحاسوب



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 37. (رقم=54)

على المستوى الوطني، تظهر ردود الدول على الاستبيان المرافق لهذه الدراسة، تباينا في الاتجاهات المستخدمة. وتفيد نسبة 70 في المائة تقريبا من الدول بأن الاستدراج يعتبر جريمة، بالرغم من أن غالبية هذه الدول تفيد بأنها تتعامل مع الاستدراج بوصفه أحد الجرائم العامة، وبالأحرى من الجرائم الخاصة في الفضاء السيبراني. بيد أن ما يزيد عن نسبة 25 في المائة تعتبر الفعل لا يمثل جريمة جنائية.

[1] Eneman, M., Gillespie, A. A., Bernd, C. S., 2010. Technology and Sexual Abuse: a Critical Review of and Internet Grooming Case. *ICIS 2010 Proceedings. Paper 144*; Kool, R., 2011. Prevention by All Means? A Legal Comparison of the Criminalization of Online Grooming and its Enforcement. *Utrecht Law Review*, 7(3):46-69.

وقد أدى تحليل المصدر الرئيسي للتشريعات المتاحة إلى تحديد أحكام خاصة تتناول استمالة الأطفال عبر الإنترنت في 17 دولة من أصل 97 دولة، حيث يقع نصف هذه الدول في أوروبا. وهذا يعكس على الأرجح تأثير الأحكام المعنية بالاستدراج في اتفاقية مجلس أوروبا لحماية الطفل وتوجيه الاتحاد الأوروبي بشأن استغلال الطفل. ومع ذلك، فإن تجريم استدراج الطفل قد تم تحديده أيضا في بعض القوانين الوطنية لدول في آسيا وأفريقيا والأمريكتين وأوقيانوسيا.

الاستدراج: مثال وطني من دولة في جنوب أوروبا

أي شخص يستعمل الإنترنت أو الهاتف أو أي وسيلة أخرى من وسائل تكنولوجيا المعلومات والاتصالات للاتصال بأحد الأشخاص تحت سن الثالثة عشر عاما وعرض عليه أن يلتقيه لارتكاب أي من الجرائم المنصوص عليها في المواد ــــــ، وبقدر ما رافق هذه الاستمالة من أفعال مادية تهدف إلى هذا المنحى، يعاقب بالسجن لمدة ــــــ عاما أو بغرامة قدرها ــــــ، وذلك بدون الإخلال بالعقوبات ذات الصلة للجرائم التي ترتكب فعلا. وتفرض العقوبات الواردة في الجزء المتقدم من القانون متى تم الحصول على المنحى بالإكراه أو التهديد أو الخداع.

الاستدراج: اتفاقية مجلس أوروبا لحماية الطفل

المادة 23 – استمالة الأطفال لأغراض جنسية

كل دولة طرف تتخذ ما يلزم من تدابير تشريعية أو تدابير أخرى لتجريم العرض المتعمد، من خلال تكنولوجيا المعلومات والاتصالات، من قبل شخص راشد للقاء طفل لم يبلغ السن المنصوص عليه في تطبيق الفقرة 2 من المادة 18 لغرض ارتكاب أي من الأفعال المجرمة وفقا للمادة 18، الفقرة 1/أ، او المادة 20 الفقرة 1/أ ضد هذا الطفل أو الطفلة، وفي حالة إذا اتبع هذا العرض بأفعال مادية تقود إلى هذا اللقاء.

جرائم حقوق المؤلف والعلامات التجارية المتعلقة بالحاسوب

يعتبر الإطار الدولي في مجال قانون الملكية الفكرية أوسع، إلى حد ما، من الإطار الافتراضي للصكوك الدولية والإقليمية المعنيتين بالجريمة السيبرانية التي عنيت بهما هذه الدراسة بشكل مباشر. وتتضمن العناصر والصكوك الرئيسية مجال قانون الملكية الفكرية، كلا من: منظمة التجارة العالمية والاتفاق المتعلق بالجوانب المتصلة بالتجارة من حقوق الملكية الفكرية[1] (والتي تضمنت لأول مرة أحكاما جنائية تتعلق بانتهاكات الحقوق التجارية للتأليف والنشر على المستوى الدولي)، علاوة على معاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية[2] ومعاهدة فناني الأداء والتسجيلات الصوتية للمنظمة العالمية للملكية الفكرية.[3] وقد صدرت في الآونة الأخيرة اتفاقية مكافحة التزوير التجاري والتي تهدف إلى ترسيخ أحكام جنائية بشأن تقليد العلامات التجارية بشكل مُتَعَمّد، أو حقوق التأليف والنشر أو النطاق التجاري للحقوق المتعلقة بانتحال مؤلفات الآخرين أو اختراعاتهم أو

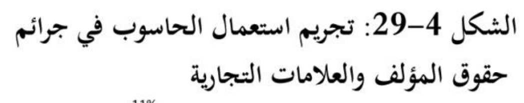
[1] الاتفاقية المتعلقة بالجوانب المتصلة بالتجارة من حقوق الملكية الفكرية، تم اعتمادها في 15نيسان/أبريل 1994.

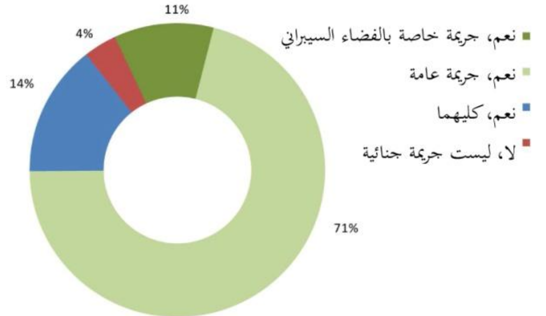
[2] معاهدة حقوق المؤلف للمنظمة العالمية للملكية الفكرية، تم اعتمادها في 20 كانون الأول/ديسمبر 1996.

[3] ومعاهدة فناني الأداء والتسجيلات الصوتية للمنظمة العالمية للملكية الفكرية، وقعت في 20 كانون الأول/ديسمبر 1996

أفكارهم أو استخدامها من غير ترخيص.[1] بيد أن البرلمان الأوروبي في عام 2012 صوت ضد هذه الاتفاقية. كما أنه من الملاحظ، أن عددا من التشريعات على مستوى دول الاتحاد الأوروبي تتناول جوانب المؤلف والحقوق المجاورة، ولكن أيا منها لا تتضمن صراحة أحكام جنائية.[2] وفي عام 2005، سن الاتحاد الأوروبي مشروع قرار وتوجيه إطاري بشأن التدابير المعنية بالأعمال الإجرامية المرتكبة ضد قانون حقوق المؤلف على نطاق تجاري.[3] وقد تم تنقيح هذا التوجيه في عام 2006، ولكن لم تتم المصادقة عليه حتى الآن.[4]

ولقد شهد العقد الماضي تطورات على المستوى الوطني تجسدت في زيادة العقوبات المقررة لجرائم حقوق التأليف والنشر، ولاسيما في حالات الأفعال الإجرامية المنظمة والتجارية. فعلى سبيل المثال، تنص اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية على تجريم التعدي على حقوق التأليف والنشر والأعمال ذات الصلة، إذا "ارتكبت بشكل متعمد" وعلى "نطاق تجاري من خلال استخدام نظام حاسوبي".[5] وفي هذا الصدد، أشارت الدول المجيبة على المستوى الوطني على الاستبيان الخاص بهذه الدراسة إلى وجود مستوى عال من تجريم الأعمال الإجرامية التي تستهدف الاعتداء على حقوق التأليف والنشر وتقليد العلامات التجارية، حيث ذكرت نسبة ما يزيد عن 80 في المائة من الدول بأن هذه الأفعال يمكن تصنيفها على أساس أنها جريمة. وجدير بالذكر، أن الغالبية العظمى من هذه الدول أفادت بأنها تستعمل الجرائم العامة بالأحرى من الجرائم الخاصة في الفضاء السيبراني.


الشكل 4-29: تجريم استعمال الحاسوب في جرائم حقوق المؤلف والعلامات التجارية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 32. (رقم=55)

غالبا ما يعني الكم الكبير من المواد المخالفة على شبكة الإنترنت (أنظر الفصل الثاني (الصورة العالمية للجريمة السيبرانية)) أن موارد إنفاذ القانون تعتبر من الناحية العملية غير كافية للملاحقة القضائية لهذا الكم الكبير من الحالات المرجّح حدوثها. ولهذا السبب، تدعم العديد من الدول أيضا المفاهيم الجديدة الواردة في إجراءات القانون المدني، مثل التحذيرات المكتوبة، ومطالبات التعويض عن الأضرار، والحق في الحصول على معلومات. بالإضافة إلى ذلك؛ فإن بعض الدول قد وضعت نماذج "لهدفين" و"ثلاثة أهداف"، حيث تلزم هذه المفاهيم

---

[1] أنظر الماد23 من اتفاقية مكافحة التزوير التجاري

[2] Sieber, U., Brüner, F.H., Satzger, H., Von Heintschel-Heinegg, B. (eds.) 2011. *Europäisches Strafrecht*, pp.442 et seq.

[3] اقتراح بشأن توجيه متعلق بتدابير جنائية تهدف إلى ضمان إنفاذ حقوق الملكية الفكرية، ومقترح بشأن قرار إطاري لتعزيز إطار القانون الجنائي لمكافحة جرائم الملكية الفكرية في الفترة من 12 آب/أغسطس 2005، اللجنة التنفيذية (2005) 276، نهائي.

[4] تعديل مشروع توجيه متعلق بتدابير جنائية تهدف إلى ضمان إنفاذ حقوق الملكية الفكرية من 2006/04/26، اللجنة التنفيذية (2006) 168، نهائي

[5] اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 10.

مقدمي خدمة الإنترنت بتسجيل عناوين بروتوكولات الإنترنت للمعتدين على حقوق التأليف والنشر بغية إرسال إخطار تحذيري للجانحين في المرة الأولى، وتحمل مسؤولية معاقبتهم عند معاودتهم لفعل ذلك مجددا، أو للتعاون من خلال إخطار أصحاب الحق أو السلطات.[1]

إستعراض

يظهر التحليل السابق أوجه التشابه والاختلافات في نُهُج التجريم الوطنية للجريمة السيبرانية. ومن الواضح، في بعض الحالات، أن الخلافات على المستوى الوطني تعتبر مماثلة أيضا لتلك على المستوى الدولي. وتتضمن أمثلة على هذه الاختلافات والتشابهات شُمُول البقاء غير القانوني في الصكوك متعددة الأطراف من عدمه، والحَدّ من عدمه، واعتراض الإرسال "غير العام"، وإمكانية تجريم "التهور" في التدخل غير القانوني في البيانات أو النظام الحاسوبي، وإدراج أو استبعاد "رموز الوصول" في الأحكام المعنية بأدوات إساءة استعمال الحاسوب. وعلى النحو الذي تم استعراضه في الفصل الثالث (الأطر والتشريعات) يشكل تَعَقّب التأثير الدقيق للصكوك الملزمة وغير الملزمة للتشريعات الوطنية تحديا واضحا. بيد أنه من الممكن في بعض الحالات تبني اتجاهين للعمل معا، وذلك كتأثير المناهج التشريعية الوطنية في تطوير الصكوك الدولية والإقليمية، والعكس صحيح. وبينما قد يبدو هذا التحليل مجرد تحليل تقني، إلا أنه اشتمل على تفاصيل المسائل المعنية بالأعمال الإجرامية التي تشكل الجريمة السيبرانية. وعلى النحو التي تمت مناقشته في الفصل السابع (التعاون الدولي)، على سبيل المثال، فإن الجوانب التفصيلية للجريمة تعتبر في بعض الدول بمثابة الأركان التي تشكلها؛ مثل "استعمال الوسائل التقنية" في ارتكاب إحدى الجرائم (على سبيل المثال، في حالة الاعتراض غير القانوني)، مما يعني أنه لا توجد جريمة بدون النص عليها. وأخيرا، فإن في هذه الظروف يمكن أن يكون لتفاصيل الجريمة تأثير على متطلبات التجريم المزدوج، بالإضافة إلى تأثيرها الفعال في التعاون الدولي.

ومن ناحية أخرى، تكشف تفاصيل التحليل النقاب عن عدد من الممارسات الجيدة في مجال تطوير القوانين الجنائية لتستوعب الأفعال التي تشكل الجريمة السيبرانية، حيث أوجد ذلك فرقا واضحا في تناول القوانين الوطنية للنفاذ غير المشروع والدخول غير القانوني في النظم الحاسوبية والبيانات الحاسوبية. وتتجسد أهمية ذلك، على سبيل المثال، في ضمان أن الأفعال المنفصلة يمكن تمييزها بشكل صحيح. علاوة على ما تقدم، فإن استخدام الظروف المشددة للعقوبة يمكن أن يكون آلية فعالة لفصل الجرائم الأساسية للشواغل الوطنية المحددة، وذلك من خلال مُرَاعاة الجرائم الأساسية التي يمكن موائمتها مع المعايير الدولية والإقليمية. ومن أجل تجنب المغالاة في التجريم، تكفل العديد من الدول أن الأحكام المعنية بأدوات إساءة استخدام الحاسوب تضمنت شرطين، أولهما أن تكون الأداة قد صممت لارتكاب جريمة، وثانيهما أن تتجه نية الجاني إلى استعمال الأداة لارتكاب هذه

[1] See Bridy, A., 2010. Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement. *Oregon Law Review*, 89:81-132; Stamatoudi, I., 2010. *Copyright Enforcement and the Internet*. Alphen aan den Rijn, Netherlands: Kluwer Law International; Haber, E., 2011. The French Revolution 2.0: Copyright and the Three Strikes Policy. *Harvard Journal of Sports & Entertainment Law,* 2(2):297-339

الجريمة. هذا، وتعتبر متطلبات الفعل المتعمد فيما يتعلق بالتدخل غير القانوني في البيانات الحاسوبية والنظم الحاسوبية من الأمور الهامة لضمان أن الأفعال التي تنطوي على إهمال أو رعونة لن تخضع لعقوبات جنائية بشكل غير متكافئ.

وأخيرا، يمثل التوازن المناسب لعملية التجريم فيما يتعلق بالجرائم ذات الصلة بالمحتوى الحاسوبي تحديا أكبر من الجرائم المرتكبة ضد السرية، والنزاهة، وتوافر بيانات حاسوبية أو نظم الحاسوب. ومن الملاحظ أنه حتى في أحد المجالات التي تناولتها المعايير الدولية مثل استغلال الأطفال في المواد الإباحية على سبيل المثال، تظهر اتجاهات الدول اختلافا فيما يتعلق بإدراج أو استبعاد مواد المحاكاة، علاوة على الفئة العمرية للطفل المحمي. وفي هذا الصدد، يعتبر القانون الدولي لحقوق الإنسان بمثابة المعيار الخارجي الأساسي الوحيد الذي يقدم توجيهات في هذا المجال. هذا، ويتناول القسم التالي من هذا الفصل المساهمة التي يمكن أن يقدمها هذا الكيان المتمثل في القانون الدولي لمساعدة الدول في تحقيق توازن مقبول بين منع الجريمة ومكافحتها وبين حماية الحريات الفردية.

3-4 القانون الدولي لحقوق الإنسان والتجريم

الاستنتاجات الرئيسية:

- ودفع الاستخدام المتزايد لوسائل التواصل الاجتماعي ومحتوى الإنترنت الذي ينتجه المستخدمون الحكومات إلى اتخاذ تدابير تنظيمية، ومن ذلك اللجوء إلى القانون الجنائي، والدعوة إلى احترام الحق في حرية التعبير
- وأبلغت البلدان المجيبة عن الاستبيان عن قيود مختلفة على التعبير، ومن ذلك القيود المفروضة على التشهير والإهانة والتهديد والتحريض على الكراهية وإهانة المشاعر الدينية والمواد الفاحشة وتقويض الدولة
- ويُجسَّد العنصر الاجتماعي والثقافي لبعض القيود ليس فقط في القانون الوطني وإنما أيضا في الصكوك متعددة الأطراف. فبعض الصكوك الإقليمية المتعلقة بالجريمة السيبرانية تشمل على سبيل المثال جرائم واسعة النطاق بشأن انتهاك الآداب العامة والمواد الإباحية والمبادئ أو القيم الدينية أو العائلية
- ويعمل القانون الدولي لحقوق الإنسان بمثابة سيف ودرع على حد سواء، إذ إنه يقضي بتجريم أشكال تعبير متطرفة (محدودة)، ويحمي أشكال تعبير أخرى. ومن ثم يتعيّن على الدول الأطراف في الصكوك الدولية لحقوق الإنسان فرض بعض القيود على حرية التعبير، بما في ذلك التحريض على الإبادة الجماعية والكراهية التي تشكّل تحريضا على التمييز أو العداء أو العنف وتحريضا على الإرهاب ودعاية للحرب
- ومن جهة أخرى، ثمة "هامش تقدير" يتيح للبلدان المجال لوضع حدود للتعبير المقبول بما يتماشى مع ثقافاتها وتقاليدها القانونية
- ومع ذلك، يكون للقانون الدولي لحقوق الإنسان دور عند نقطة معينة. فتطبيق القوانين الجنائية المتعلقة بالتشهير وعدم احترام السلطة والإهانة مثلا على التعبير على الإنترنت، سيواجه صعوبات كبيرة لإثبات تناسب التدابير وملاءمتها واتّساقها بأقل قدر من التدخل
- وعندما يكون المحتوى غير قانوني في بلد ما، ويكون إنتاجه ونشره قانونيا في بلد آخر، سيتعين على الدول التركيز في تدابير العدالة الجنائية التي ستتخذها على الأشخاص الذين يطّلعون على المحتوى الذي يعدّ غير قانوني ضمن ولايتها القضائية الوطنية، بدلا من التركيز على المحتوى المنتج خارج البلد

ينص القانون الدولي لحقوق الإنسان على تجريم مجالات الجريمة السيبرانية ويحظرها. وقد تم تطوير الفقه القانوني المتعلق بحرية التعبير بشكل خاص لمساعدة الدول على وضع حدود حول تجريم التعبير في مجالات متنوعة مثل خطاب الكراهية والتحريض على الإرهاب، والتشهير، والفحش والإهانة.

حقوق الإنسان بمثابة "سيف" و"درع"

منذ أكثر من ثلاثين عاما، ذكر رئيس لجنة الأمم المتحدة لمنع الجريمة ومكافحتها وقتئذ أن: "الجريمة تعتبر كذلك إذا عرفها القانون على هذا النحو.[1] ومن ناحية أخرى، يجب أن يراعي التعريف وجود حقوق الإنسان واحترامها، ولا تكن مجرد تعبير عن سلطة تعسفية".[2] وبعبارة أخرى؛ لا تعتبر القوانين الجنائية الوطنية بمنأى عن إشراف القانون الدولي لحقوق الإنسان.[3]

مع بعض الاستثناءات الوَجِيهة (مثل الالتزام باعتبار كل أفعال التعذيب بمثابة جريمة جنائية، وحظر الأثر الرجعي للجرائم الجنائية)،[4] فإن القانون الدولي لحقوق الإنسان لم يحدد بشكل مباشر وعلى نحو تقليدي ما يجب أو ما لا يجب اعتباره جريمة جنائية في القانون الوطني.[5] وبالرغم من ذلك، فإن الفقه القانوني المعني بالقانون الدولي لحقوق الإنسان يواجه بشكل متزايد تساؤلا عما إذا كان تجريم سلوك مُعَيّن يعتبر متوافقا مع حقوق الإنسان الفردية، أو حتى يقتضي ذلك. وفي الاضطلاع بذلك، فإن القانون الدولي لحقوق الإنسان يعتبر "درعا" و"سيفا"، فإما تحييد القانون الجنائي أو إطلاقه.[6]

---

[1] تأسست اللجنة بموجب قرار المجلس الاقتصادي والاجتماعي للأمم المتحدة في أيار/مايو 1971. أنظر قرار المجلس الاقتصادي والاجتماعي للأمم المتحدة رقم 1548 (L) 1971.

[2] López-Rey, M., 1978. Crime and Human Rights. *Federal Probation* 43(1):10-15, p.11.

[3] ولأغراض هذه الدراسة؛ تعتبر حقوق الإنسان الواردة في القانون الدولي الإنساني، المعاهدات التسعة الأساسية المعنية بحقوق الإنسان وبروتوكولاتهم، فضلا عن آليات المعاهدات الثلاثة الإقليمية، والتفسيرات الرسمية لهذه الصكوك من قبل الآليات المنشأة بموجبه، أو خلاف ذلك لأغراض تعزيزهم وتنفيذهم، قد اتخذت كتعبير أساسي مرادفا "للقانون الدولي لحقوق الإنسان"، ويشتمل ذلك على: العهد الدولي الخاص بالحقوق المدنية والسياسية، العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري، اتفاقية القضاء على جميع أشكال التمييز ضد المرأة، اتفاقية مناهضة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة، اتفاقية حقوق الطفل، الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم، الاتفاقية الدولية لحماية جميع الأشخاص من الاختفاء القسري، واتفاقية حقوق الأشخاص ذوي الإعاقة. بالإضافة إلى البرتوكولات الاختيارية لكل من العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، العهد الدولي الخاص بالحقوق المدنية والسياسية، اتفاقية القضاء على جميع أشكال التمييز ضد المرأة، اتفاقية حقوق الطفل، اتفاقية مناهضة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة، واتفاقية حقوق الأشخاص ذوي الإعاقة، وتغطي مجالات مثل إلغاء عقوبة الإعدام (العهد الدولي الخاص بالحقوق المدنية والسياسية-البرتوكول الاختياري الثاني)، انخراط الأطفال في النزاعات المسلحة (البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن اشتراك الأطفال في المنازعات المسلحة)، وبيع الأطفال واستغلالهم في البغاء، علاوة على استغلالهم في المواد الإباحية (البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية) (أيضا تم إدراج الجريمة السيبرانية كأحد الصكوك في هذه الدراسة). فعلى المستوى الإقليمي، تتضمن الاتفاقية الدولية لحماية جميع الأشخاص من الاختفاء القسري والخمسة عشر برتوكولا الملحقين بها، ويشتمل ذلك على حماية الملكيات والحق في التعليم وحرية التنقل، إلغاء عقوبة الإعدام، وحظر عام على التمييز، المجلس الاستشاري لحقوق الإنسان في الأمريكتين وأفريقيا، والمجلس الاستشاري لحقوق الإنسان. وفي الوقت الحالي لا توجد أي اتفاقيات على مستوى آسيا في مجال حقوق الإنسان.

[4] المادة (4) من اتفاقية مناهضة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة، والمادة 15 (1) من العهد الدولي الخاص بالحقوق المدنية والسياسية.

[5] ومع ذلك، تجدر الإشارة إلى أن القانون الدولي لحقوق الإنسان يشترط تعويضات لانتهاكات حقوق الإنسان، وقد يشتمل هذا بدوره على سن قوانين جنائية مناسبة كافية للردع والرد على الانتهاكات المحددة.

[6] Tulkens, F., 2011. The Paradoxical Relationship between Criminal Law and Human Rights. *Journal of International Criminal Justice,* 9(3):577-595

بينما لدى الدولة الطرف في معاهدات حقوق الإنسان التزام بوضع نظم وقوانين جنائية كافية للردع والرد على الهجمات ضد الأفراد،[1] إلا أنه يجب ألا نذهب بعيدا إلى حد إنكار الحقوق الفردية عن طريق تجريمها لسلوك معين.[2] وعند إجراء هذا التقييم، يجب تقييم الحكم الوارد في القانون الجنائي على أساس "كل حق على حدة"،[3] وذلك لفحص ما إذا كان محتوى الحكم ينتهك مجموعة من الحقوق الفردية، مثل الحق في عدم التعرض لتدخل تعسفي أو غير قانوني في الخصوصية أو العائلة أو المنزل أو المراسلات،[4] وكذلك الحق في حرية الفكر والمعتقد والدين،[5] أو الحق في التجمع السلمي.[6]

تحقيق التوازن

كثيرا ما يتطلب مثل هذا التقييم من الهيئات الدولية لحقوق الإنسان أن تتَدَبّر بعناية عددا من المصالح. حيث لا تعتبر العديد من الأحكام الواردة في القانون الدولي لحقوق الإنسان مطلقة. فعلى سبيل المثال: قد تخضع الحقوق المتعلقة بحرية الفكر، والرأي والدين، والتعبير، والتجمع إلى قيود (بما في ذلك القيود الواردة في القانون الجنائي)[7] تبدو ضرورية لمجموعة من المصالح، منها الأمن القومي، والسلامة العامة، والنظام العام، وحماية الصحة العامة أو صيانة الأخلاق العامة أو حماية حقوق الآخرين وحرياتهم.[8]

إن التدخل المسموح في حقوق الإنسان يجب أن يكون عادة: (1) منصوص عليه في القانون أو وفقا لما يقتضيه القانون؛ (2) متوافق مع الأهداف المشروعة؛ (3) ضروريا في مجتمع ديمقراطي.[9] وفي تحديد ماهية حالة الضرورة – في السياق الأوروبي– ترى المحكمة الأوروبية لحقوق الإنسان إذا ما كان التدخل يعتبر متوافقا لتحديد حاجة اجتماعية اضطرارية.[10] وقد منحت الدولة "هامشا من التقدير" في هذا الصدد.[1] ويعتبر الهامش الممنوح بمثابة "سياق مَشْرُوط"، ولاسيما فيما يتعلق بطبيعة الحق المعني والهدف المتوخى من التدخل لمتابعته.

---

[1] أنظر على سبيل المثال: المحكمة الأوروبية لحقوق الإنسان، التماس رقم 94/23452. 28 تشرين الأول/أكتوبر 1998، حيث انتهت المحكمة إلى أن الحق في الحياة (المحكمة الأوروبية لحقوق الإنسان المادة الثانية الفقرة الأول)، تتضمن الالتزام بوضع (أحكام جنائية فعالة لردع ارتكاب الجرائم ضد الأشخاص مدعومة بآلية إنفاذ القانون لمنع ومكافحة انتهاكات هذه الأحكام فضلا عن العقوبات المقررة لذلك).

[2] لجنة الأمم المتحدة المعنية بالمخدرات ولجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية، 2010، المخدرات ومنع الجريمة والعدالة الجنائية: منظور حقوق الإنسان. مذكرة من المدير التنفيذي:E/CN.7/2010/CRP.6 – E/CN.15/2010/CRP.1. 3 March 2010

[3] المرجع السابق.

[4] المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

[5] المادة 18 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

[6] المادة 21 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

[7] فقد توصلت المحكمة الأوروبية لحقوق الإنسان إلى أن وجود حظر جنائي لسلوك معين يعتبر كافيا للتدخل المستمر في حقوق الإنسان (تتعلق هذه الحالة بالحق في الحياة) حتى عندما توجد سياسة ثابتة بعدم تحريك الدعوى الجنائية. أُنظر المحكمة الأوروبية لحقوق الإنسان. الطلب رقم 89/15070. 22 نيسان/أبريل 1993.

[8] المادة 21 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

[9] أُنظر على سبيل المثال: الصياغات المستخدمة في الاتفاقية الأوروبية لحقوق الإنسان، المواد 8-11.

المحكمة الأوروبية لحقوق الانسان، الطلب رقم 72/5493. 7 كانون الأول/ديسمبر 1976.

[10] المحكمة الأوروبية لحقوق الانسان، الطلب رقم 72/5493. 7 كانون الأول/ديسمبر 1976.

الجريمة السيبرانية – حقوق الإنسان والقانون الجنائي

يسري تأثير "الدرع" و"السيف" للقانون الدولي لحقوق الإنسان أيضا على تجريم أفعال الجريمة السيبرانية، حيث تقدم الأخيرة مجالا واسعا للتجريم، يشتمل على تجريم الأفعال ضد السرية، والنزاهة، وتوافر بيانات حاسوبية أو نظم حاسوب، واستخدام الحاسوب لتحقيق مكاسب مالية أو شخصية أو تسبب ضررا، والأفعال المتعلقة بالمحتوى الحاسوبي. وتجدر الإشارة إلى أن بعضا من هذه الأحكام الجنائية قد ترتبط بالالتزامات الواردة في القانون الدولي لحقوق الإنسان إلى حد كبير أكثر من غيرها.

ومن الممكن أن ترتبط الجرائم المتصلة بالمحتوى الحاسوبي بشكل خاص بحقوق تعاهدية، مثل الحق في حرية التعبير،[2] والحقوق ذات الصلة بالممتلكات،[3] والتزامات الدول المقررة لضمان أمن الأشخاص وحمايتهم من الإيذاء البدني.[4] ويخضع المحتوى المتاح عبر الإنترنت إلى نظام حقوق الإنسان البادِئُ ذِكْرُهُ، باعتباره من حيث المبدأ كوسيط إعلامي تقليدي، مثل المواد والمحَادَثَات المطبوعة. وباستقراء قرار مجلس حقوق الإنسان التابع للأمم المتحدة رقم 8/20، فإنه يؤكد على أن "ذات الحقوق المقررة للناس دون الاتصال بالإنترنت يجب حمايتها أيضا عبر الإنترنت، ولاسيما حرية التعبير والتي تنطبق بغض النظر عن الحدود ومن خلال أي وسيلة إعلامية من اختيار أي شخص.[5]

بالرغم من ذلك، فإن *المحتوى* عبر الإنترنت لديه سمات خاصة، بما في ذلك حقيقة أن تأثير وطول بقاء المعلومات يمكن مضاعفتها متى وضعت على الإنترنت، حيث يعتبر الوصول للمحتوى من الأمور البسيطة للقصّر. ولقد بدأت التطويرات في شبكات التواصل الاجتماعي، ومحتوى الإنترنت الذي ينتجه المستخدمون تشكل تحديا للاحتكارات التقليدية بشأن المعلومات.[6] وكنتيجة لذلك، يجب أن يؤخذ في الاعتبار عند تفسير الأحكام المعنية بحقوق الإنسان الطبيعة الخاصة لشبكة الإنترنت باعتبارها أحد وسائل نَقْل المعلومات.[7]

---

1 For a general review, see Legg, A., 2012. *The Margin of Appreciation in International Human Rights Law*. Oxford: Oxford Monographs in International Law

2 المادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية، المادة 9 من الاتفاقية الأوروبية لحقوق الإنسان، المادة 13 من الاتفاقية الأمريكية لحقوق الإنسان، والمادة 9 من الميثاق الأفريقي لحقوق الإنسان والشعوب

3 المادة 1 من البرتوكول الأول المرافق للاتفاقية الأوروبية لحقوق الإنسان، المادة 21 من الاتفاقية الأمريكية لحقوق الإنسان، والمادة 14 من الميثاق الأفريقي لحقوق الإنسان والشعوب.

4 المواد من 4-17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، المواد من 3-8 من الاتفاقية الأوروبية لحقوق الإنسان، المواد 5، و11 من الاتفاقية الأمريكية لحقوق الإنسان، والمادة 5 من الميثاق الأفريقي لحقوق الإنسان والشعوب.

5 مجلس حقوق الإنسان التابع للأمم المتحدة، 2012، قرار رقم 8/20 بشأن تعزيز وحماية والتمتع بحقوق الإنسان على شبكة الإنترنت، 16تموز/ يوليو 2012. A/HRC/RES/20/8

6 مجلس الأمم المتحدة لحقوق الإنسان، 2012. ملخص للنقاش مجلس حقوق الإنسان المعني بتعزيز وحماية حرية التعبير على الإنترنت. تقرير مكتب مفوض الأمم المتحدة السامي لحقوق الإنسان. 2 تموز/يوليو 2012، A/HRC/21/30

7 المحكمة الأوروبية لحقوق الإنسان، قسم البحوث 2011، الإنترنت: السوابق القضائية الصادرة عن المحكمة الأوروبية لحقوق الإنسان

الجريمة السيبرانية والحق في حرية التعبير

لقد أظهر عدد من القضايا البارزة مؤخرا، بالإضافة إلى أداء آليات حقوق الإنسان على المستوى الدولي والإقليمي،[1] مدى أهمية حرية التعبير على الإنترنت. وقد سُئلت الدول خلال جمع المعلومات عن كيفية حماية القانون لحرية التعبير في شكله الإلكتروني، كما طُلب منها تحديد ما إذا كان يجوز تقييد حرية التعبير لأغراض منع أو مكافحة الجريمة السيبرانية، وتحت أي ظرف من الظروف يمكن أن يتم ذلك.

وقد أشارت كل الدول تقريبا التي أجابت على هذا السؤال (نحو 50 دولة) إلى أن حرية التعبير بشكل عام تعتبر محمية- عادة بموجب الدستور- وتسري هذه الحماية بشكل متساوٍ على التعبير الإلكتروني وغير الإلكتروني.[2] أيضا، وأشار عدد من الدول إلى القوانين "بشأن المعلومات"، وقوانين "الصحافة والنشر"، وقوانين "الوسائل المرئية والمسموعة"، وقوانين "وسائل الإعلام" تتضمن حمايات مناسبة.[3]

حرية التعبير على الإنترنت – نموذج حالة

في تشرين الثاني/نوفمبر 2011، قضت محكمة العدل الأوروبية بأن لا يجوز أن يُطلب من مقدمي خدمة الإنترنت تنقّية المحتوى لأغراض إنفاذ حقوق المؤلف والنشر، حيث ينتهك ذلك حقوق المشتركين في الخصوصية، وحرية التعبير. وطبقا للمحكمة، فإن إلزام مقدمي الخدمة بتصفية المحتوى لا يتعارض فقط مع توجيه الاتحاد الأوروبي بشأن التجارة الإلكترونية، بل يعتبر انتهاكا للحقوق الأساسية لعملاء مقدمي خدمة الإنترنت، أي حقوقهم في حماية بياناتهم الشخصية وحريتهم في إرسال واستقبال المعلومات... [أولا]، قد ينطوي أمر الإلزام بتركيب نظام لتنقية المحتوى المتنازع عليه على تحليل منهجي لكافة المحتوى وجمع وتحديد عناوين بروتوكولات الإنترنت للمستخدمين مما يعتبر بمثابة إرسال للمحتوى غير القانوني عبر الشبكة. [ثانيا]، من المحتمل أن يقوض هذا الأمر حرية الإعلام بِحَيْثُ لا يميز هذا النظام بشكل ملائم بين المحتوى القانوني والمحتوى غير القانوني، مما قد ينجم عنه حجب الاتصالات المشروعة. ولقد أقامت إدارة إحدى الشركات التي تمثل مبدعي المصنفات الموسيقية والتي لها الحق في الترخيص باستخدام المواد المحمية بحقوق هؤلاء المبدعين الخاصة بالتأليف والنشر من قِبَل الغير دعوى قضائية ضد أحد موزعي خدمة الإنترنت الذي يوفر الوصول إلى الإنترنت بدون تقديم خدمات أخرى مثل تبادل الملفات أو تحميلها. وقد طلبت الشركة من موزع خدمة الإنترنت أن يضطلع بالرقابة، وبالتالي حجب التواصل لنقل الملفات المعنية بمواد أنتجها عملاء أوروبيون قد اضطلعت الشركة بتمثيلهم أمام المحكمة.

المصدر: محكمة العدل الأوروبية، القضية رقم C-70/10

وفيما يتعلق بالقيود المفروضة على حرية التعبير، أشارت الدول المجيبة على الاستبيان إلى مجموعة واسعة من القيود المحتملة، حيث اشتملت على القيود العامة الواردة في القانون الدولي لحقوق الإنسان، مثل تلك الرامية إلى حماية "الأمن القومي"،

---

[1] أنظر على سبيل المثال، المقرر الخاص للأمم المتحدة حول حرية الرأي والتعبير، وممثل منظمة الأمن والتعاون في أوروبا بشأن حرية وسائل الإعلام، والمقرر الخاص لمنظمة الدول الأمريكية بشأن حرية التعبير، والمقرر الخاص للميثاق الأفريقي لحقوق الإنسان والشعوب بشأن حرية التعبير والوصول إلى المعلومات. إعلان مشترك حول حرية التعبير والإنترنت، متاح على الرابط التالي: http://www.osce.org/fom/78309

[2] الاستبيان الخاص بهذه الدراسة، السؤال رقم 20.

[3] المرجع السابق.

والسلامة العامة ومنع الفوضى أو الجريمة"، و"النظام العام"، و"الصحة العامة"، و"الآداب والأخلاق العامة". كما تضمنت قيودا أكثر تحديدا، مثل: "انتهاك السرية"، و"ميزة قانونية"، و"القذف"، و"تهديد الأشخاص أو الممتلكات"، و"التحريض على الجريمة"، و"المساعدة المادية للإرهاب"، و"الدعاية للحرب"، و"التحريض على الإبادة الجماعية"، و"التحريض على الكراهية القومية أو العنصرية أو الدينية"، و"إهانة المشاعر الدينية"، و"ازدراء الأديان المحمية أو ذمها أو التَجْرِيح فيها"، و"المواد التي تقوض العلاقات المتَسَاوِقة بين الشعوب والطوائف والقبائل والمجتمعات"، و"الفُحْش"، و"الإباحية"، و"النيل من هيبة الدولة أو تَقْوِيض الثقة في الوضع المالي للدولة"، وأخيرا "نشر الأسرار الرسمية".[1]

اعتبر عدد من الدول القانون الدولي والإقليمي بمثابة المصدر لبعض من هذه القيود المفروضة، ومنها القرار الإطاري لمجلس الاتحاد الأوروبي بشأن مكافحة العنصرية وكراهية الأجانب،[2] وكذلك برتوكول مجلس أوروبا المرافق لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.[3] بيد أن الدول الأخرى اعتبرت القوانين الوطنية فقط بمثابة مرجعتيها. وفي هذا الصدد، فقد قدم عدد من الدول معلومات تتعلق بالطريقة التي بموجبها تحدد شرعية القيود.[4] ومع ذلك، فإن أغلب الدول لم تقدم معلومات بشأن النهج المستخدم في تحديد شرعية القيود المفروضة على حرية التعبير. ومن ناحية أخرى، فقد أوضحت بعض الدول أن القيود المحددة على حرية التعبير انبثقت من المحظورات الجنائية. وبشكل عام؛ مع ذلك، لم تحدد الدول المجيبة على الاستبيان الخاص بهذه الدراسة ماهية طبيعة القيود المفروضة، إذا كانت جنائية أو مدنية أو إدارية.

القيود على حرية التعبير والقانون الدولي

إن بعض القيود المفروضة على حرية التعبير – التي أشارت إليها الدول المجيبة – تحظى بدرجة عالية من الدعم من القانون الدولي لحقوق الإنسان. تتطلب وظيفة "السيف" للقانون الدولي لحقوق الإنسان، في أشكاله القصوى، حظر (تقييد) أشكال محددة من التعبير. ويحدد المقرر الخاص للأمم المتحدة المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، أربعة أشكال من التعبير يجب حظرها بموجب القانون الدولي لحقوق الإنسان: استغلال

[1] المرجع السابق

[2] القرار الإطاري لمجلس الاتحاد الأوروبي 2008/913/JHA الصادر في 28 تشرين الثاني/نوفمبر 2008 بشأن مكافحة أشكال ومظاهر العنصرية وكراهية الأجانب من خلال وسائل القانون الجنائي OJ L 328، 6 كانون الأول/ديسمبر 2008.

[3] تتطلب المواد من 3 إلى 6 من برتوكول مجلس أوروبا المرافق لاتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، من الدول الأعضاء اعتماد تدابير تشريعية وتدابير أخرى إذا اقتضى الأمر ذلك، لاعتبار نشر المواد المتعلقة بالعنصرية وكراهية الأجانب من خلال نظم الحاسوب، أو التهديدات ذات الدوافع العنصرية أو المعادية للأجانب، أو الإهانات التي تنطوي على عنصرية كراهية للأجانب بمثابة جريمة جنائية. بالإضافة إلى إنكار أو التقليل الجسيم أو الموافقة على أو تبرير الإبادة الجماعية أو إنكارها أو التقليل من جسامتها أو الموافقة عليه، إلى جانب ذلك الجرائم ضد الإنسانة.

[4] ذكرت أحد الدول الأفريقية، على سبيل المثال، أن الحقوق الواردة في ميثاق الحقوق قد تكون مقيدة فقط في سياق التطبيق العام للقانون إلى الحد الذي يعتبر معه أن هذه القيود مسببة أو مبررة في مجتمع ديمقراطي ومنفتح قائم على الكرامة الإنسانية والمساواة والحرية، مع مراعاة كل العوامل ذات الصلة، بما فيها (أ). طبيعة الحقوق، (ب) أهمية الغرض من القيد المفروض، (ج) وسائل تقليل حد الحقوق المقيّدة لتحقيق الغرض. الاستبيان الخاص بهذه الدراسة، السؤال رقم 20.

الأطفال في المواد الإباحية،[1] التحريض المباشر والعلني على ارتكاب جرائم الإبادة الجماعية،[2] والدعوة إلى الكراهية القومية أو العرقية أو الدينية والتي تشكل تحريضا على التمييز أو العداوة أو العنف،[3] والتحريض على الإرهاب.[4] هذا، وقد أضاف المقرر الخاص الدعاية للحرب.[5] وكما هو مبين أدناه، فإن القيود الأخرى المفروضة على حرية الرأي تحظى بدعم أقل في إطار القانون الدولي لحقوق الإنسان.

يفصل الجدول عددا من الأحكام المعنية بحقوق الإنسان والحالات، وفقا للنتائج المترتبة على ما إذا كان التجريم يعتبر *مطلوبا* أو *مقبولا* أو *غير مطلوب*، أو من المحتمل *ألا يتوافق* مع القانون الدولي لحقوق الإنسان. ويبرز الجدول أنه يجوز للدول، على الأقل في ظل الولاية القضائية الدولية المتاحة، أن تقيد حرية التعبير بشكل مشروع متى انطوت على خطاب كراهية أو فحش. ومن ناحية أخرى، فإن القيود التي تعتبر أكثر من اللازم بشكل كبير أو التي تفتقر إلى اليقين القانوني أو التي تحد من النِقاش التعدّدي قد تتعارض مع المعايير الدولية لحقوق الإنسان. وفي هذا السياق، يعمل القانون الدولي الإنساني كدرع واقٍ ضد المغالاة في التجريم.

التجريم المطلوب من جانب القانون الدولي لحقوق الإنسان
الفقرة (2) من المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية، المادة 4 من الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري، والمادة 13 من الاتفاقية الأمريكية لحقوق الإنسان. أية دعوة إلى [الكراهية القومية أو العنصرية أو الدينية تشكل تحريضا على التمييز أو العداوة أو العنف (العهد الدولي الخاص بالحقوق المدنية والسياسية)]، [العنف غير القانوني أو أي من الأفعال المماثلة الأخرى (الاتفاقية الأمريكية لحقوق الإنسان)] [التحريض على التمييز العنصري أو وكل عمل من أعمال العنف ضد أي عرق أو أية جماعة من لون أو أصل أثني آخر (الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري)]، ويتعين [حظرها بموجب القانون (العهد الدولي الخاص بالحقوق المدنية والسياسية)]، [وتعتبر بمثابة جرائم يعاقب عليها القانون (الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري، والاتفاقية الأمريكية لحقوق الإنسان)].
البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية، المادة 3 يتعين أن يتناول القانون الجنائي أو قانون العقوبات بشكل كلي إنتاج أو توزيع أو نشر أو استيراد أو تصدير أو عرض أو بيع أو حيازة مواد إباحية متعلقة بالطفل على النحو المذكور أعلاه، وسواء أكانت هذه الجرائم ترتكب محليّا أو دوليّا أو كانت ترتكب على أساس فردي أو منظم.
الفقرة (1) من المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية، والمادة 13 من الاتفاقية الأمريكية لحقوق الإنسان أي دعاية للحرب [يتعين حظرها بموجب القانون (العهد الدولي الخاص بالحقوق المدنية والسياسية)] / [واعتبارها إحدى الجرائم المعاقب عليها بموجب القانون (الاتفاقية الأمريكية لحقوق الإنسان)].
التجريم المقبول وفقا لقرارات حقوق الإنسان

[1] الأمم المتحدة، البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال واستغلال الأطفال في البغاء وفي المواد الإباحية، المادة 3.

[2] اتفاقية منع جريمة الإبادة الجماعية المادة 3، النظام الأساسي للمحكمة الجنائية الدولية الفقرة3/ه المادة25، النظام الأساسي للمحكمة الجنائية الدولية ليوغوسلافيا السابقة الفقرة 3/ج، المادة 4، النظام الأساسي للمحكمة الجنائية الدولية لرواندا الفقرة ج/3، المادة 2.

[3] العهد الدولي الخاص للحقوق المدنية والسياسية، الفقرة2، المادة 20

[4] قرار مجلس الأمن للأمم المتحدة رقم 1624 (2005)،(2005) Para 1.S/RES/1624 14 أيلول/ سبتمبر 2005.

[5] العهد الدولي الخاص للحقوق المدنية والسياسية، الفقرة 1، المادة 20

المحكمة الأوروبية لحقوق الإنسان. الالتماس رقم 03/5446
لا تعتبر إدانة نشر مواد تندرج تحت أفعال الفحش عبر الإنترنت انتهاكا للحق في حرية التعبير. بِالرّغْمِ مِنْ أنّ المادة قد تعتبر مشروعة في بلد آخر حيث يخضع تسيير مواقع الإنترنت فيها إلى الرقابة. ولم يجادل مقدم الالتماس في أن المادة كانت بذيئة وفقا للقانون، وانتهت المحكمة إلى أن التدخل كان متناسبا مع الأخذ بعين الاعتبار الطبيعة التجارية للموقع على شبكة الإنترنت.
المحكمة الأوروبية لحقوق الإنسان. الالتماس رقم 05/10883
لا تعتبر إدانة التحريض على التمييز القومي أو العرقي أو الديني النَاتِج عَنْ التصريحات التي أدلى بها رئيس بلدية المدينة أو المنشورة على الموقع الشبكي لمجلس البلدية انتهاك للحق في حرية التعبير، حيث طالبت التصريحات بمقاطعة المنتجات من إحدى الدول الأخرى. وقضت المحكمة أن التدخل قد يكون ذا صلة وكافيا، مع الأخذ في الاعتبار المنصب العمومي الذي يشغله مقدم الطلب.
التجريم غير المطلوب وفقا لقرارات حقوق الإنسان
المحكمة الأوروبية لحقوق الإنسان. الالتماس رقم 03/31358
لا تعتبر دولة المدعي عليه ملتزمة بإجراء تحقيق في أحد الشكاوى المقدمة إلى الشرطة بشأن استلام رسائل إلكترونية طفيلية غير مرغوب فيها، نظرا لأن القانوني الجنائي المعمول به لا يتناول هذا السلوك.
قيود التجريم وفقا لقرارات حقوق الإنسان
المحكمة الأوروبية لحقوق الإنسان. الالتماس 07/13290
تعتبر الإدانة الجنائية لقذف موظف عمومي عبر التعليقات المنشورة على أحد مواقع الإنترنت حول قرارات الموظف المسؤول بمثابة تدخل غير متجانس مع الحق في حرية التعبير. وقد قضت المحكمة بأنه يجب أن يكون لدى المسؤولين المنتخبين قدر من التسامح فيما يتعلق بالنقد الموجه إليهم علاوة على التجاوزات اللفظية التي قد ترافق النقد في بعض الأحيان.
الأمم المتحدة – اللجنة المعنية بحقوق الإنسان البلاغ رقم CCPR/C/103/D/1815/2008
خلصت اللجنة إلى أن إدانة أحد المذيعين العاملين في الراديو بتهمة القذف تشكل قيدا غير مشروع على الحق في حرية الرأي. وأوضحت اللجنة أنه يتعين أن تتضمن هذه القوانين دفاعا عن الحقيقة، ولا ينبغي سريانها على حرية التعبير التي لا يجوز أن تخضع للتحقيق.
المحكمة الأوروبية لحقوق الإنسان. الالتماس رقم 07/2034
الإدانة الجنائية "للإهانة الجسيمة ضد الملك" تعتبر تدخلا غير متجانس مع الحق في حرية التعبير. وأشارت المحكمة إلى أن هذا الجزاء بطبيعته سيكون له حتما تأثير سلبي.
الأمم المتحدة – اللجنة المعنية بحقوق الإنسان البلاغ رقم CCPR/C/85/D/1180/2003
انتهت اللجنة إلى أن إدانة مقدم الطلب للسَبّ الجنائي الوارد في أحد المقالات بشأن زعيم إحدى الجماعات الحزبية تمثل تدخلا غير متجانس مع الحق في حرية التعبير. وذكرت اللجنة أن القيمة التي وضعها العهد الدولي بشأن التعبير الإباحّي، تعتبر للشخصيات في المجال السياسي مرتفعة بشكل خاص.
المحكمة الأوروبية لحقوق الإنسان. الالتماس رقم 07/27520
يعتبر تَجْرِيم "تشويه سمعة الوطن، الجمهورية، الجمعية الوطنية الكبرى، وحكومة الجمهورية أو الأجهزة القضائية للدولة" تدخلا غير متكافئ مع الحق في حرية التعبير. ولاحظت المحكمة أن المصطلح كان ذا نطاق ضيق وغامض، ولا يمكن الأفراد من تنظيم سلوكهم أو الأخذ بعين الاعتبار عواقب أفعالهم.
المحكمة الأوروبية لحقوق الإنسان. الالتماس رقم 97/35071
يعتبر تَجْرِيم "التحريض على الكراهية والعداء على أساس الطبقة الاجتماعية، أو العرق، أو الدين، أو المذهب، أو القومية" الوارد في التعليقات التي تنتقد المبادئ الديمقراطية وتدعو إلى فرض الشريعة تدخلا غير متكافئ مع الحق في حرية التعبير. وانتهت المحكمة إلى أن تلك التعليقات قد أُبديت في سياق نقاشات تعددية.

تنص المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية – على المستوى الدولي – على أنه: "تحظر بالقانون أية دعوة إلى الكراهية القومية أو العنصرية أو الدينية تشكل تحريضا على التمييز أو العداوة أو العنف".[1] وردا على السؤال بشأن تجريم استخدام الحاسوب في الأفعال التي تنطوي على عنصرية أو كراهية الأجانب، أفادت ثلاثة أرباع الدول المجيبة على الاستبيان بأن ذلك يعتبر من قبيل الجرائم الجنائية الموجودة، غير أن باقي الدول ذكرت بأنه هذه الأفعال لا تشكل جريمة.[2]

فإذا تم تجريم هذه الأفعال، فإن أغلبية الجرائم تُصنف كجرائم عامة، بدلا من جرائم خاصة في الفضاء السيبراني. وتظهر الاتجاهات المتبعة للتجريم في هذا المجال مساحة كبيرة من التَنَوّع. فبعض الدول لديها جرائم تتناول التحريض على الكراهية العرقية والدينية، في حين أن دولا أخرى لديها جرائم تتناول فقط الأفعال المتعلقة بالكراهية العرقية أو الإثنية.[3] وتتمثل المواقف التي تدعم مجموعة من القيود الضيقة فقط في الخطاب الذي يهدف إلى "توليد خوف من الضرر المستقبلي" إلى

خطاب الكراهية: مثال وطني من دولة في أوروبا الغربية

التحريض على الكراهية

(1) أي شخص يسلك طريقا من شأنه أن يعمل على تكدير السلم العام

1. يحرض على الكراهية ضد شرائح من السكان أو يدعو إلى اتخاذ إجراءات عنيفة أو تعسفية ضدهم؛ أو

2. يعتدي على الكرامة الإنسانية للآخرين من خلال إهانتهم أو قذفهم، أو التشهير بهم، يعاقب بالسجن لمدة تتراوح من ثلاثة شهور إلى خمس سنوات.

(2) أي شخص:

1. فيما يتعلق بمواد مكتوبة تتضمن تحريضا على الكراهية ضد شريحة من شرائح المجتمع أو جماعة وطنية أو عرقية أو دينية أو أي فرد متسم بعادته العرقية والذي يدعو إلى استعمال العنف أو التعسف ضدهم، أو تتضمن هذه المواد المكتوبة تحريضا على الاعتداء على الكرامة الإنسانية للآخرين من خلال إهانتهم أو قذفهم، أو التشهير بهم أو مجموعة سبق الإشارة إليها

(أ) نشر هذه المواد المكتوبة؛

(ب) عرض هذه المواد علنا أو تعليقها أو عرضها أو يجعلها متاحة في متناول الجميع؛

(ج) يقدم، أو يدعم، أو يجعل هذه المواد في متناول أي شخص دون الثامنة عشر؛

(د) ينتج أو يحصل أو يدعم أو يشهر أو يعلن أو يوصي أو يتعهد باستيراد أو تصدير هذه المواد المكتوبة لاستخدامها أو نسخها لتحقيق المعنى الوارد في الفقرات أ إلى جـ أو تسهيل هذا الاستخدام من قبل شخص آخر؛ أو

2. نشر عرض لمحتوى مشار إليه في البند 1 أعلاه من خلال الراديو أو وسائل الإعلام أو خدمات الاتصال

يعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو غرامة مالية. ...

[1] ينبغي ملاحظة أن المادة 20 من العهد الدولي لم تشترط التجريم، بل مجرد حظر بموجب القانون. بيد أن الاتفاقية الأمريكية لحقوق الإنسان الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري اشترطا أن تعتبر هذه الدعوات بمثابة جرائم يعاقب عليها القانون.

[2] الاستبيان الخاص بهذه الدراسة، السؤال رقم 35.

[3] مكتب الأمم المتحدة للمفوض السامي لحقوق الإنسان، 2012. خطة عمل الرباط بشأن حظر الدعوة إلى الكراهية القومية أو العنصرية أو الدينية التي تشكل تحريضا على التمييز أو العداوة أو العنف. الاستنتاجات والتوصيات المنبثقة عن حلقات عمل الخبراء الإقليمية الأربعة التي نظمتها مفوضية حقوق الإنسان، في عام 2011، واعتمدت من قبل خبراء في الرباط، المغرب في 5 أكتوبر/تشرين الأول عام 2012.

توسيع نطاق التجريم ليشمل "الإدلاء بتصريحات مهينة" حول مجموعة من الأشخاص على أساس العرق أو الدين أو المعتقد أو الجنس أو التوجه الجنسي أو الإعاقة.[1]

لقد أدى تزايد استخدام شبكات التواصل الاجتماعي إلى ظهور عدد من الحالات مؤخرا عبر شبكة الإنترنت تثير القضايا المتعلقة بخطاب الكراهية، بما في ذلك المواد المرئية (فيديو) تتضمن محتويات معادية للإسلام ورسائل تحرض على العنصرية عبر توتير.[2] وبينما تفرض المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية التزاما لمكافحة مثل هذه التعابير، إلا أنه من الهام تَذَكّر أن المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية تتطلب مستوى عاليا، حيث يجب أن تستوفي القيود المفروضة مقياسا لثلاثة أجزاء: الشرعية والتناسب والضرورة. ويتعين عند تّقييم شدة الكراهية، ومن ثم تبرير القيود المفروضة على حرية التعبير، أن يتضمن مستوى التقييم: (أ) سياق البيان، (ب) وضع وحالة المتكلم، (ج) النية (يتعين ألا يعتبر الإهمال والتهور كافِيا)، (د) محتوى البيان أو شكله، (هـ) نطاق البيان، (و) درجة الخطر الناتج عن الضرر.[3] تستجلي المبادئ غير الملزمة أن مصطلحي "الكراهية" و" العَدَاوَة" قد استعملا في المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية، حيث تشير إلى " مجموعة مكثفة من العواطف غير المنطقية متعلقة بالازدراء والعداوة والمقْت تجاه مجموعة مستهدفة".[4] وعلى المستوى الأوروبي؛ فإن المحكمة الأوروبية لحقوق الإنسان تؤكد على الحاجة إلى حَثّ حقيقي وجادّ ضد التطرف بدلا من الأفكار التي ببساطة تسيء إلى الآخرين وتزعجهم أو تَرَوّعهم.[5]

فعندما يتعلق الأمر "بالكراهية الدينية" بشكل خاص، فإن لجنة حقوق الإنسان التابعة للأمم المتحدة تؤكد على أن المحظورات بشأن العروض التي تظهر في "عدم احترام أي دين من الأديان أو نظم المعتقدات الأخرى، بما في ذلك قوانين التكفير" تعتبر مُخَالِفة لِلعهد الدولي الخاص بالحقوق المدنية والسياسية، فيما عدا الشروط المتوخاة في المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية.[6] فعلى سبيل المثال، تلاحظ

---

[1] منظمة الأمن والتعاون في أوروبا 2011، حرية التعبير عبر الإنترنت: دراسة الأحكام والممارسات القانونية المتعلقة بحرية التعبير وحرية تدفق المعلومات والتعددية الإعلامية على شبكة الإنترنت في الدول المشاركة في المنظمة؛ هالبين أس 2010، خطاب الكراهية العنصري: دراسة تحليلية مقارنة لتأثير القانون الدولي لحقوق الإنسان على قانون المملكة المتحدة والولايات المتحدة. استعراض قانون ماركيه، 94 (2): 463-497.

[2] أنظر الى سبيل المثال:

http://www.bbc.co.uk/news/world-middle-east-19606155 and http://www.bbc.co.uk/news/uk-england-gloucestershire-20560496

[3] مكتب الأمم المتحدة للمفوض السامي لحقوق الإنسان، 2012. خطة عمل الرباط بشأن حظر الدعوة إلى الكراهية القومية أو العنصرية أو الدينية التي تشكل تحريضا على التمييز أو العداوة أو العنف. الاستنتاجات والتوصيات المنبثقة عن حلقات عمل الخبراء الإقليمية الأربعة التي نظمتها مفوضية حقوق الإنسان، في عام 2011، واعتمدت من قبل خبراء في الرباط، المغرب في 5 أكتوبر/تشرين الأول عام 2012.

[4] المادة 19. 2009، مبادئ كادمن بشأن حرية التعبير والمساواة، المبدأ 12

[5] مجلس أوروبا، 2012 صحيفة الوقائع-خطاب الكراهية

[6] لجنة حقوق الإنسان التابعة للأمم المتحدة، 2011. تعليق عام رقم 34. المادة 19 من حرية الرأي والتعبير CCPR/C/GC/34 12 أيلول/سبتمبر 2011، الفقرة 48.

اللجنة أنه قد لا يُسمح باستعمال هذه المحظورات "لمنع أو معاقبة انتقاد الزعماء الدينيين أو التعليق على العقيدة الدينية والمبادئ العقائدية".[1]

التحريض على الإرهاب

طالب عدد من الصكوك على المستوى الدولي والإقليمي الدول بأن تحظر التحريض على الإرهاب، وقد استخدمت حيال ذلك لغة تمثلت في "التحريض العلني على ارتكاب إحدى الجرائم الإرهابية"، أو "التحريض على ارتكاب عمل إرهابي".[2] وعندما سُألت هذه الدول عن تجريم دعم الجرائم الإرهابية (بما في ذلك؛ استعمال الحاسوب في التحريض على الإرهاب)، أفادت نسبة 90 في المائة تقريبا بوجود الجرائم ذات الصلة بالإرهاب. وفي حالة اعتبار أن هذه الأفعال مجرمة، فإن ما يقرب من نسبة 80 في المائة من الدول أفادت بأنها قد استخدمت "أحد الجرائم العامة"، بيد أن نسبة 15 في المائة فقط أفادت بوجود جرائم خاصة بدعم بالإرهاب في الفضاء السيبراني، أما النسبة الباقية (5 في المائة) من الدول أفادت بأنها تستخدم كل من الجرائم العامة والجرائم الخاصة في الفضاء السيبراني.[3]

وباستقراء الواقع، فإن خطاب الكراهية وشبكة الإنترنت وشبكات التواصل الاجتماعي أنشأت منابر جديدة، واسعة النطاق، للتحريض على الإرهاب.[4] وحيث إن الحكومات تضطلع بتطبيق القوانين الحالية ووضع قوانين جديدة على غرار من نشره مكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن استعمال شبكة الإنترنت للأغراض الإرهابية، فمن الأهمية بمكان أن تقر الدول توازنا مناسبا بين متطلبات إنفاذ القانون وبين حماية حقوق الإنسان والحريات في هذا المجال.[5] وتظهر التقارير التي سلمتها الدول الأعضاء إلى لجنة مكافحة الإرهاب في الأمم المتحدة بشأن تنفيذ مجلس الأمن رقم 1624 (2005) تَنَوّعا كبيرا في طريقة حظر وتعريف التشريعات الوطنية لماهية التحريض على الإرهاب.[6] وبشكل خاص، فإن الاستجابات الوطنية يمكن أن تتضمن أو تستبعد أعمالا أوسع نطاقا مثل تبرير الأفعال الإرهابية أو الثناء عليها.[7]

---

[1] المرجع السابق.

[2] أنظر على سبيل المثال، اتفاقية مجلس أوروبا بشأن مكافحة الإرهاب، المادة 5، والقرار الإطاري لمجلس دول الاتحاد الأوروبي 2002/475/JHA الصادر في 28 تشرين الثاني/نوفمبر 2002 بشأن مكافحة الإرهاب (بصيغته المعدلة من قِبَل والقرار الإطاري لمجلس دول الاتحاد الأوروبي 2008/919/JHA الصادر في 28 تشرين الثاني/نوفمبر 2008) المادة 3، وقرار مجلس الأمن للأمم المتحدة رقم 1624 (2005) ,(2005) 1.S/RES/1624 14 أيلول/سبتمبر 2005

[3] الاستبيان الخاص بالدراسة، السؤال رقم 38

[4] See, for example, http://www.justice.gov/opa/pr/2011/February/11-nsd-238.html and http://www.cps.gov.uk/news/press_releases/137_07/

[5] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012، استخدام الإنترنت لأغراض إرهابية، ص 41

[6] تقارير الدول الأعضاء بشأن التدابير المتخذة لحظر التحريض على الإرهاب بموجب القانون ومنع ارتكاب أي فعل من الأفعال الإرهابية. متاحا على الرابط التالي: http://www.un.org/en/sc/ctc/resources/1624.html.

أنظر ايضا كموجز عام:
For an overview, see also van Ginkel, B., 2011. Incitement to Terrorism: A Matter of Prevention or Repression? *ICCT Research Paper*. The Hague: International Centre for Counter-Terrorism.

[7] المرجع السابق، وأنظر أيضا، التقارير المقدمة من قبل البرازيل ومصر، ولاتفيا، وإسبانيا، والمملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية.

قد يشكل استخدام مصطلحات مُلْتَبِسة – من منظور حقوق الإنسان – مثل "تقديس" أو "تشجيع" الإرهاب إشكالية عند وضع قيود على حرية التعبير،[1] حيث أن مفهوم "التقديس"، قد لا يكون مصطلحا ذو مفهوم ضيق بشكل كاف أو مَضْبُوط ليكون أساسا لفرض عقوبات جنائية متوافقة مع متطلبات مبدأ المشروعية. وبالأحرى، فإن مصطلح التحريض يمكن أن يفهم منه بأنه دعوة مباشرة للانخراط في الإرهاب، مع توافر نية أن هذا الانخراط يعزز الإرهاب، إلى جانب أن سياق الدعوة المباشرة قد تكون سببا مسؤولا عن تصاعد إمكانية وقوع عمل إرهابي فعلي.[2] وبشكل خاص، يقترح المقرر الخاص للأمم المتحدة المعني بتعزيز وحماية الحق في حرية الرأي والتعبير أن الصياغة الواردة في قرار مجلس الأمن رقم 1624 (2005) (حظر التحريض على ارتكاب عمل إرهابي أو أعمال أخرى بموجب القانون) تمثل أفضل معالجة مناسبة للموقف المعني باعتبار أن توزيع رسالة بشكل متعمد وغير مشروع أو جعلها متاحة إلى الجمهور بنية التحريض على ارتكاب أحد الأعمال الإرهابية، يعتبر جريمة، وكذلك في حالة إذا تسبب السلوك – سواء كان التحريض صراحة لارتكاب جرائم إرهابية من عدمه – في وجود خطر قد يتيح ارتكاب جريمة أو أكثر".[3]

التحريض على الإرهاب – نموذج حالة

في عام 2011، قد أُتهم شاب يبلغ من العمر 22 عاما من مواطني أحد دول أمريكا الشمالية بتورطه في توزيع معلومات تتعلق بمُتَفَجّرات، وتوجيه نداء لارتكاب العنف على أرض البلاد. هذا، وقد وجهت إليه تهمة إضافية تضمنت الاعتداء على أحد ضباط إنفاذ القانون، وحيازة سلاح ناري للتَشْجِيع ارتكاب إحدى جرائم العنف. وكان المتهم أحد المديرين النشطاء، المعروفين دوليا، لأحد المواقع الإسلامية المتطرفة، حيث وضع عددا من المنشورات التي تعبر عن ميوله للآراء المتطرفة، وذلك بالتزامن مع تجشيع الأعضاء الأخرين باتباع عقيدته للإشراك في ارتكاب جرائم عنف في أمريكا الشمالية ضد أهداف مثل أقسام الشرطة، ومكاتب البريد، والمعابد، والمنشآت العسكرية، ومرافق النقل. ولأجل دعم هذه الهجمات، قام المتهم أيضا بنشر رابط إلكتروني لوثيقة مطولة تحتوي على خطوات تفصيلية عن كيفية تصنيع المتفجرات. وقد أدين المتهم بالتحريض على جرائم العنف وحيازة سلاح ناري لدعم أحد جرائم العنف، وذلك في صيف عام 2011، وبالرغم من صدور الحكم ضده، إلى أن قرارا صدر بإعادة إدراج الدعوى حتى كانون الثاني/يناير 2013.

الأشكال الأخرى للتعبير وتحدي التقاليد القانونية والولاية القضائية

من المستقر، أن هناك عادة أشكالا أخرى للتعبيرات المحظورة؛ توجد بشكل مُتَشَابِه ولكن بنسبة أقل في التوافق بين القوانين الوطنية والاتجاهات الدولية والإقليمية. وقد أشار عدد من الدول–في جميع مناطق العالم –

[1] الجمعية العامة للأمم المتحدة، 2008. وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب. تقرير الأمين العام A/63/337، 28 آب/أغسطس 2008.

[2] المرجع السابق

[3] الجمعية العامة للأمم المتحدة، 2011. تعزيز وحماية الحق في حرية الرأي والتعبير. تقرير المقرر الخاص A/66/290، 10 آب/أغسطس 2011.

أثناء جمع المعلومات الخاصة بهذه الدراسة، إلى تأثير القوانين الجنائية العامة على حرية الرأي، بما في ذلك: السب والقذف، والفحش، والمواد الإباحية، والحض على الفجور، والآداب العامة، والمنشورات غير المرغوب فيها.[1]

وعلى اعتبار أن الإنترنت وشبكات التواصل الاجتماعي أصبحت من الأمور الهامة في مجال النشاط السياسي والتعبير الثقافي والاجتماعي، فإن ذلك يرافقه حاجة ناشئة لكل من (1) تصنيفات وطنية فيما يتعلق بأشكال التعبير عبر الإنترنت التي يسري عليها القانون الجنائي، (2) مناقشة تتعلق بتجريم الأمور المختلفة التي تنجم عن المسائل القضائية والأعراف القانونية المختلفة.

وفي إطار مواجهة التصاعد الكبير "للجرائم"[2] الناجمة عن استعمال شبكات التواصل الاجتماعي، فقد أصدرت بعض الدول مؤخرا، على سبيل المثال، إرشادات مَرْحَلِيّة بشأن الملاحقة القضائية للحالات التي تنطوي على رسائل مرسلة عبر شبكات التواصل الاجتماعي.[3] وتؤكد هذه الإرشادات التوجيهية على أنه يجب تفسير الأحكام الجنائية بما يتوافق مع مبادئ حرية التعبير، علاوة على إمكانية أن يساعد تفسير هذه الأحكام في توضيح نطاق التعبيرات المقبولة. وفي هذا الصدد، يسمح "هامش التقدير" لمبدأ حقوق الإنسان بمنح الدول مُهْلَة محددة تضطلع خلالها بتحديد ماهية التعبيرات المقبولة التي تتماشى مع ثقافاتها وتقاليدها القانونية،[4] رغم أن القانون الدولي لحقوق الإنسان قد يتدخل عند نقطة معينة. هذا، وقد وجدت لجنة حقوق الإنسان التابعة للأمم المتحدة أن قوانين القذف الجنائي، على سبيل المثال، قد تنتهك حقوق حرية التعبير، مما يستوجب أن تتضمن هذه القوانين دفاعات مثل الدفاع عن الحقيقة.[5] وقد أعربت اللجنة أيضا عن قلقها إزاء القوانين المعنية بمسائل مثل:

---

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 34، 36، و39

[2] في إنجلترا وويلز، على سبيل المثال، في عام 2008، كانت هناك تقارير تقدر بـ 556 بشأن مزاعم حول جرائم ارتكبت عبر شبكات التواصل الاجتماعي والمتهم فيها 46 شخص. وفي 2012، كان يوجد عدد 4.908 تقرير يتهم 653 شخص. أُنظر:

http://www.bbc.co.uk/news/uk-20851797، وفي غرب آسيا تم الإبلاغ عن عدد من القضايا الجنائية الحديثة تتعلق بمحتوى شبكة الإنترنت وشبكة التواصل الاجتماعي، أنظر http://www.bbc.co.uk/news/world-middle-east-20587246

[3] دائرة الادعاء الملكية، 2012، المبادئ التوجيهية المؤقتة لملاحقة الحالات التي تنطوي على الرسائل الموجهة عبر وسائل التواصل الاجتماعي. الصادرة عن مدير النيابة العامة، 19كانون الأول/ ديسمبر 2012.

[4] في حالة إذا كانت أحد الحقوق أو القيم الهامة بشكل خاص تعتبر على المحك، فإن هامش التقدير الممنوح لأحد الدول سيتم تقييده، بشكل عام (المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 04/44362. 18 نيسان/أبريل 2006). وعلى النقيض من ذلك، إذا كان الهدف المنشود لا يحظى بإجماع عالمي–مثل المقصود بـ"حماية الأخلاق العامة". سيتم توسيع نطاق هامش التقدير في هذه الحالة (المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 84/10737. 24 أيار/مايو 1988). هذا، وتوظف المحكمة الأوروبية لحقوق الإنسان، من بين أمور أخرى، معيار التوافق (الأوروبي) المشترك في تحديد الهامش المتاح، حيث يتم توسيع هامش تقدير عند غياب توافق الأرداء بشأن المعني أو الحاجة إلى فرض قيود على حقوق معينة. وعلى العكس من ذلك، ففي وجود توافق الآراء، يؤخذ معنى المفهوم "الأساسي" للحق مما يُصّعب تعريف هذا الحق، إلى جانب تعديل هامش التعهدات. وبالتالي، فإن هامش التقدير الداخلي يسير جنبا إلى جنب مع "إشراف الأوروبيين"، وذلك فيما يتعلق بكل من الهدف من التدخل و"الضرورة" التي تستوجب ذلك. إن مبدأ هامش التقدير يعتبر أقل تطورا في أداء محكمة البلدان الأمريكية لحقوق الإنسان ولجنة حقوق الإنسان التابعة للأمم المتحدة. وبالرغم من ذلك، يفيد المعلقون أن هناك تصاعد لدور هامش التقدير في منظومة البلدان الأمريكية، بالإضافة إلى أن مَسْأَلَة أشكال المبْدَأ يدعم بالأدلة الكثيرة، حيث يعتبر جزء من ممارسة لجنة حقوق الإنسان التابعة للأمم المتحدة (Legg, A., 2012، هامش التقدير في القانون الدولي لحقوق الإنسان. أكسفورد: أكسفورد الدراسات التخصصية في القانون الدولي)

[5] United Nations Human Rights Committee Communication CCPR/C/85/D/1180/2003 and United Nations Human Rights Committee, 2011. *General Comment No. 34*. Article 19: Freedoms of opinion and expression. CCPR/C/GC/34, 12 September 2011. para. 47.

الطعن في الذات الملكية، وانتهاك حرمة المحكمة، وعدم احترام السلطة، وعدم احترام العلم والرموز، والتشهير برئيس الدولة، وحماية شرف الموظفين العموميين.[1]

وعندما يتعلق الأمر بالمحتوى العالمي للإنترنت، فإن قضايا مثل بيرين (Perrin)[2] والرابطة الدولية لمناهضة العنصرية ومعاداة السامية (LICRA) ضد شركة ياهو،[3] تسلط الضوء على الصعوبات التي تُثار في حالة إذا كان محتوى الإنترنت يعتبر مقبولا ومُوَلّدا في إحدى الدول، بينما يعتبر متاحا في دولة أخرى. ففي قضية "برين"، على سبيل المثال، وجدت المحكمة الأوروبية لحقوق الإنسان أن تطبيق قوانين مكافحة الفحش في دولة المدعي عليه على محتوى الإنترنت في أحد المواقع الإلكترونية والذي يتم تشغيله والتحكم فيه في دولة ثالثة، وفي حالة إذا كان المحتوى غير قانوني، فإن ذلك لا يعتبر تجاوزا لهامش التقدير الخاص بدولة المدعي عليه.[4] ولقد أدلى المعلقون برأيهم في هذه القضية، حيث قالوا إن المحكمة الأوروبية طبقت هامش التقدير بشكل مفرط ولم يحالفها التوفيق في التصدي بشكل كاف للمسائل القضائية، وتمثل ذلك في إجَازَة المحكمة لنطاق قضائي عريض بصورة كامنة للدول على منتجي المحتوى في دول أخرى طبقا لمعايير المحتوى الخاصة بهم.[5] ولم تتناول المحكمة، على سبيل المثال، التقارب أو الروابط من ناحية أخرى بين مقدم الطلب (الشركة المالكة للموقع والتي يقع مقرها في دولة أخرى) وبين دولة المدعي عليه.[6] وفي هذا الصدد، أوصى الإعلان المشترك بشأن الآليات الدولية لتعزيز حرية التعبير، وحرية التعبير عبر الإنترنت بأنه يتعين تقييد الولاية القضائية في الحالات القانونية ذات الصلة بمحتوى الإنترنت على "الدول التي لديها اتصال حقيقي وجوهري بهذه الحالات". ويعتبر ذلك "من الأمور الاعتيادية بسبب أن صاحب البلاغ قد أنشأ هناك المحتوى الحقيقي الذي تم تحميله هناك أيضا و/أو ووجه المحتوى بشكل خاص إلى تلك الدولة".[7]

---

[1] المرجع السابق، فقرة 38

[2] المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 04/5446

[3] وفي قضية الرابطة الدولية لمناهضة العنصرية ومعاداة السامية ضد شركة ياهو، أمرت المحكمة الوطنية شركة ياهو بأن تتخذ الإجراءات لمنع المستخدمين في تلك الدولة من الوصول إلى أحد المواقع الخاصة بالمزاد ومقرها في دولة ثالثة حيث كان يتم بيع أشياء تذكارية تخص العهد النازي ((Ordonnance de référérendue le 20 Novembre 2000. Tribunal de grande Instance de Paris. No. RG : 00/05308). وفي الإجراءات اللاحقة في الدولة المستضيف للموقع الإلكتروني، قضت أحد المحاكم الوطنية في الطعن المقدم بأنه لا توجد أسباب لمنح الولاية القضائية إلا إذا تم تنفيذ الحكم القضائي الأجنبي أمام المحاكم الوطنية، كما أن التذرع بحرية التعبير لا يجوز بالتالي أن تكون بمثابة أمر من الأمور المسلية في تلك الوقت *Yahoo Inc. v La Ligue Contre le Racisme et l'Antisemitisme.* (No. 01-17424. United States Court of Appeals, Ninth Circuit.)

[4] المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 04/5446

[5] مجلس أوروبا، مفوضية حقوق الإنسان، 2012، وسائل التواصل الاجتماعي وحقوق الإنسان. إصدار ورقة نقاشيةComm DH ، 08 شباط/فبراير 2012

[6] المرجع السابق، ص 17

[7] المقرر الخاص للأمم المتحدة المعني بحرية الرأي والتعبير، ممثل الجماعات الاقتصادية لدول غرب أفريقيا بشأن حرية الإعلام، المقرر الخاص منظمة البلدان الأمريكية بشأن حرية التعبير، والمقرر الخاص الميثاق الأفريقي لحقوق الإنسان والشعوب بشأن حرية التعبير والوصول إلى المعلومات. الإعلان المشترك بشأن حرية التعبير والإنترنت. متاح على الرابط التالي: http://www.osce.org/fom/78309

وبشكل عام؛ يمكن للقانون الدولي لحقوق الإنسان أن يستوعب النهج الوطنية المتباينة لتجريم محتوى الإنترنت أو محتوى شبكات التواصل الاجتماعي، ضمن حدود مُقَرّرة. ويتضمن ذلك، المحظورات الجنائية المبَاحة بشأن استغلال الطفل في المواد الإباحية، والتحريض المباشر والعلني على ارتكاب الإبادة الجماعية، والدعوة إلى الكراهية القومية أو العرقية أو الدينية والتي تشكل تحريضا على التمييز أو العداوة أو العنف، أو التحريض على الإرهاب أو الدعاية للحرب. مع ذلك، فإن الجرائم الجنائية ذات الصلة بالقذف، والمواد البذيئة، والإهانة، من المرجح أن تصطدم بأحد الحدود العالية، حتى في نطاق هامش التقدير، والتي تبرهن على أن التدابير تتوافق مع مبدأ التناسب، مما يعتبر مناسبا لتحقيق وظائفها الوِقَائِيّة، إلى جانب ذلك، فإن هذه التدابير تعتبر على الأقل بمثابة الأداة المتَدَخّلة من بين تلك التي يمكن من خلالها تحقيق الحماية.[1]

"يتعين على المدعيين العامين أن يراعو أن هناك اختلافا بين السياق التفاعلي للمحادثات التي تجرى عبر شبكات التواصل الاجتماعي، والسياق الذي يحدث عبر الاتصالات الأخرى...
قد تصل اتصالات منوي إرسالها إلى قليلين، إلى الملايين، ولهذا السبب، ينبغي للمدعين العامين الشروع في تحريك الدعوى الجنائية فقط في حالة إذا تحققوا أن الرسائل محل البلاغ تعتبر أكثر من عدوانية أو صادمة أو مزعجة، أو تَهَكّمِيّة أو تحض على التمرد، أو وقحة أو تتضمن عبارات مكروهة، أو آراء غريبة بشأن مسائل خطيرة أو تافِه، أو مُدَاعَبَة أو فُكَاهَة، حتى لو كانت بَغِيضة للبعض أو مؤلمة للذين يتلقونها."

مبادئ توجيهية بشأن الملاحقة القضائية للحالات التي تنطوي على الرسائل الموجهة عبر وسائل التواصل الاجتماعي (دولة في شمال أوروبا)

علاوة على ما تقدم؛ فإذا حاولت الدول فرض الولاية القضائية على المحتوى الحاسوبي تأسيسا على معاييرها الوطنية، فمن المرجح أن يبلور القانون الدولي بشكل متزايد أحد الاحتياجات لإثبات أن المحتوى الذي تم إنشاءه أو استضافته في دول أخرى يعتبر بشكل خاص مستهدفا لأشخاص داخل دولة التطبيق أو الوصول لهم بشكل متكرر. فإذا كان المحتوى غير مشروع في إحدى الدول، ولكن يعتبر إنتاجه ونشره مشروعا في دولة أخرى، فإن القانون الدولي لحقوق الإنسان، باعتباره الدرع والسيف، يقدم في هذه الحالة أداة هامة تساعد في تعيين التعابير المقبولة. وفي هذا الصدد، تقوم نظم حقوق الإنسان الدولية والإقليمية بتطوير فقهها القانوني على الأقل في بعض المجالات ومن ناحية أخرى فإنه من المحتمل أن يُمَكّن "التوافق" بشأن أحد حقوق الإنسان من تَوَجّيه حجم هامش التقدير على المستوى الدولي. وختاما، إذا كانت الاختلافات الوطنية لا يمكن التقريب بينها في نهاية المطاف، فمن المرجح أن تحتاج الدول التركيز على استجابات العدالة الجنائية بشأن الأشخاص الذي يصلون للمحتوى الحاسوبي ضمن سياق ولايتهم القضائية الوطنية، بدلا من التركيز على منتجي المحتوى خارج نطاق الولاية القضائية الوطنية.

[1] لجنة حقوق الإنسان التابعة للأمم المتحدة 2011، التعليق العام رقم 34، المادة 19 حرية التعبير والرأي CCPR/C/GC/34 12 أيلول/سبتمبر 2011، الفقرة 34.

الفصل الخامس: إنفاذ القانون والتحقيقات

يتناول هذا الفصل السلطات المسؤولة عن إنفاذ القانون والتحقيقات بشأن الجريمة السيبرانية وفقا لمجموعة من وجهات النظر، تشتمل على، الصلاحيات القانونية لتدابير التحقيق، ومَسْألَة ضمانات الخصوصية، والتحديات التي تواجه التحقيقات، والممارسات الجيدة، والتفاعل بين إنفاذ القانون والقطاع الخاص، بالإضافة إلى قدرات السلطات المعنية بإنفاذ القانون وتدريبها. مما يبرهن على التعقيدات التي تعترض التحقيقات في الجريمة السيبرانية، والحاجة إلى أطر قانونية فعّالة، والجمع بين موارد إنفاذ القانون والمهارات العملية.

1-5 إنفاذ القانون والجريمة السيبرانية

الاستنتاجات الرئيسية

- أشار أكثر من 90 في المائة من البلدان المجيبة عن الاستبيان إلى أنَّ السلطات المسؤولة عن إنفاذ القانون تبلَّغ بمعظم الجرائم السيبرانية من خلال البلاغات المقدّمة من الضحايا الأفراد أو الضحايا من الشركات
- وقدَّرت البلدان المجيبة عن الاستبيان أنَّ نسبة التأذّي الفعلي من الجريمة السيبرانية المبلّغ عنها إلى الشرطة تبدأ من واحد في المائة. وتشير دراسة استقصائية عالمية للقطاع الخاص إلى أنَّ 80 في المائة من الضحايا الأفراد للجرائم السيبرانية الأساسية لا يبلغون الشرطة عن الجريمة
- تهدف سلطات إنفاذ القانون إلى التصدي إلى تدني الإبلاغ عن هذه الجرائم من خلال مجموعة من التدابير تتضمن التوعية ورفع الوعي
- يجب أن تقترن تدابير التصدِّي للجريمة السيبرانية التي تتخذ لمعالجة حوادث معينة، بتحقيقات استراتيجية على المدى المتوسط والبعيد، تركز على أسواق الجريمة ومدبري المخططات الإجرامية
- تعتبر نسبة الكشف عن أفعال الجريمة السيبرانية من خلال التحقيقات الاستباقية منخفضا، بيد أن عددا من الدول تركز على العمليات الاستراتيجية السرية

دور إنفاذ القانون

تسلط المادة 1 من مدوَّنة الأمم المتحدة لقواعد سلوك الموظفين المكلفين بإنفاذ القوانين[1] على أن دور الموظفين المكلفين بإنفاذ القوانين يتجسد في أداء الواجب المفروض عليهم "من خلال خدمة المجتمع"، و"حماية جميع الأشخاص من الأفعال غير المشروعة". بيد أن هذا الواجب الوظيفي يمتد ليتشمل على مجموعة من المحظورات الواردة في القوانين الجزائية.[2] وفي إطار انتشار أفعال الجريمة السيبرانية،[3] فإن أجهزة إنفاذ القانون تواجه بشكل متزايد سؤالا يتعلق بماهية المقصود بـ "يخدم"، و"يحمي" في سياق جريمة ذات أبعاد عالمية.

وقد تبين خلال جمع المعلومات الخاصة بهذه الدراسة أن أكثر من نصف الدول أفادت أن ما بين 50 و100 في المائة من أفعال الجريمة السيبرانية تواجه من قِبَل الشرطة عندما تنطوي هذه الأفعال على أحد عناصر الجريمة عبر الوطنية.[4] وفي نفس الوقت؛ أشارت الدول المجيبة على الاستبيان الخاص بهذه الدراسة إلى أن غالبية أفعال الجريمة السيبرانية تلتفت إليها الشرطة من خلال البلاغات الفردية للمجني عليهم. وبِالتّالِي فإن الجريمة السيبرانية تأخذ المنحى العالمي، ولكن تتمثل البلاغات المقدمة في وقوعها على المستوى المحلي. وقد يصل البلاغ إلى أحد الخطوط الوطنية الساخنة أو أحد الوحدات الشرطية المتخصصة، ولكن قد يصل أيضا إلى أحد مكاتب الشرطة الريفية أو المحلية الأكثر اعتيادا على التعامل مع الجرائم التقليدية "كالسطو المسلح"، أو "السرقة"، أو "السَلْب"، أو "القتل". ومع ذلك، وعلى غرار الجريمة "التقليدية"، يعتبر كل من ضحايا الجريمة السيبرانية ومرتكبو الجريمة السيبرانية أفرادا حقيقيين متواجدين في أماكن جغرافية حقيقية، كما يقع كليهما ضمن اختصاص إحدى دوائر الشرطة المحلية.

وفي كثير من الأحيان، ترسل أقسام الشرطة المحلية قضايا الجريمة السيبرانية إلى إحدى هيئات إنفاذ القانون المتخصصة على المستوى الوطني. ومع ذلك؛ فمن المتوقع أن يقود تنامي تدخل الأدلة الإلكترونية في كل أنواع الجرائم إلى إحداث ثَوْرَة في التقنيات الشرطية في العقود المقبلة سواء على المستوى المركزي أو المحلي. ففي بعض الدول، على سبيل المثال، تُجهز بشكل روتيني أقسام الشرطة المحلية بتكنولوجيا مكتبية لاستخراج بيانات الهواتف المحمولة من المشتبه بهم.[5] وفي هذا الصدد؛ تسلط الدول المجيبة على الاستبيان الخاص بهذه الدراسة الضوء على التفاوت الكبير في قدرة قوات الشرطة للاضطلاع بالتحقيق في الجريمة السيبرانية سواء إذا كانت الجرائم داخل الدولة أو عبر الحدود الوطنية. ومن الملاحظ أن إحدى الدول أفادت بأن: "هناك تفاوت كبير بين مقرات هيئة

---

[1] مدوَّنة الأمم المتحدة لقواعد سلوك الموظفين المكلفين بإنفاذ القوانين، المادة الأولى. الملحق المرافق لقرار الجمعية العامة للأمم المتحدة رقم 169/34، 17كانون الأول/ديسمبر 1979

[2] المرجع السابق، التعليق على المادة (1)، فقرة (د).

[3] أنظر الفصل الثاني (الصورة العالمية للجريمة السيبرانية).

[4] الاستبيان الخاص بهذه الدراسة، السؤال رقم 83. بعض الدول التي لم تتمكن من تقديم أرقام دقيقة، يتوقع أن تكون النسبة عالية جدا.

[5] See http://www.bbc.co.uk/news/technology-18102793

الشرطة بعضها البعض عندما يتعلق الأمر بجريمة سيبرانية، فبعض منها لديه وحدات متخصصة على علم جيد بمثل هذه الجرائم، في حين أن لدى أقسام الشرطة الأخرى يكاد يوجد عدد قليل من الضباط المدربين".[1]

ومع ذلك، يجب أن ترافق إجراءات للجريمة السيبرانية التي تتخذ لمعالجة حوادث معينة، بتحقيقات استراتيجية على المدى المتوسط والبعيد، تركز على أسواق الجريمة وتقديم مدبري المخططات الإجرامية إلى العدالة. وغني عن البيان؛ أن مكافحة أي شكل من أشكال الجريمة يتطلب اتباع نهج استباقي موجه لحل مشاكل حفظ الأمن والنظام العام، حيث تعمل الشرطة جنبا إلى جنب مع الشركاء الآخرين متعددي الاختصاصات[2] نحو هدف عام يتمثل في المحافظة على النظام الاجتماعي والسلامة العامة.[3]

وتتطلب مفاهيم الشرطة عن "المجتمع" المرتبط "بالسلامة العامة" أن تنتقل هذه المفاهيم من عالم غير متصل بالإنترنت إلى عالم متصل بالإنترنت. وبالرغم من ذلك؛ ترى الدول المجيبة على الاستبيان الخاص بهذه الدراسة أن هذا يعتبر بمثابة مبدأ يجب أن يسري بصورة متساوية على حد السواء عندما يتعلق الأمر بجريمة سيبرانية، وذلك فضلا عن العديد من عناصر الممارسات الجيدة للشرطة في منع الجريمة التقليدية. وهذه الأمور تتطلب بشكل خاص حاجة هيئات إنفاذ القانون للعمل مع القطاع الخاص والشركات من منظمات المجتمع المدني، علاوة على تطبيق حفظ الأمن والنظام العام المستند إلى معلومات استخباراتية لمنع ومكافحة الجريمة السيبرانية بشكل استباقي، واستخدام مناهج حل الإشكاليات القائمة على المعلومات الدقيقة واستكشاف الآفاق. ومن الملاحظ أن إحدى الدول أفادت بأن: "الهجمات أصبحت أكثر تقدما وأكثر صعوبة للكشف عنها، وفي الوقت نفسه تجد التقنيات طريقها بسرعة إلى جمهور أوسع".[4]

وعلى النحو المذكور في هذا الفصل؛ فإن العناصر الحيوية لأحد تحركات هيئات إنفاذ القانون التَوَافُقِيّة لمواجهة أفعال الجريمة السيبرانية المبلّغ عنها، تتضمن بالتالي: (1) إطارا قانونيا فعّالا لتدابير التحقيق يعمل على إيجاد توازن مناسب بين احترام الخصوصية الفردية وصلاحيات التحقيق، (2) الوصول إلى أدوات وتقنيات التحقيق بشكل عملي، بما في ذلك وسائل الحصول على الأدلة الإلكترونية من الأطراف الثلاثة، مثل: موزعي خدمة الإنترنت، (3) القدرات التقنية والتدريب الكافي للضبَّاط المتخصصين وغير المتخصصين.

ماهية الفعل الذي تتصدى له أجهزة الشرطة

خلال جمع المعلومات الخاصة بهذه الدراسة، ذكرت الدول المجيبة على الاستبيان بأن ما يزيد عن 90 في المائة من الأفعال التي تصل إلى علم الشرطة، تأتي من خلال البلاغات المقدمة من الضحايا الأفراد أو الضحايا

---

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 113.

[2] مكتب الأمم المتحدة المعني بالمخدرات والجريمة 2010، كتيب عن المبادئ التوجيهية لمنع الجريمة: العمل بموجبها.

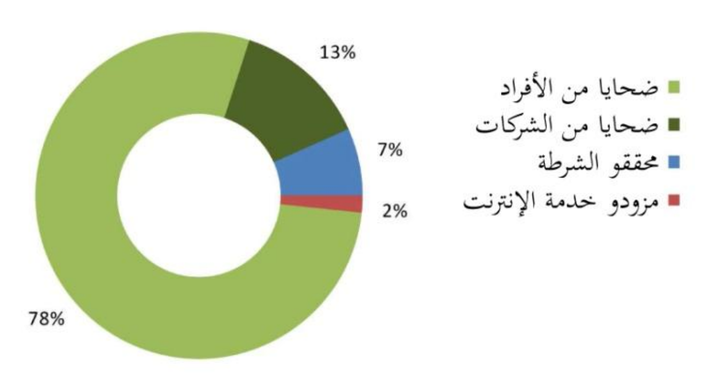
[3] Bowling, B., and Foster, J., 2002. Policing and the Police. *In*: Maguire, M., Morgan, R., Reiner, R. (eds.). *The Oxford Handbook of Criminology*. 3rd edn. Oxford: Oxford University Press.

[4] الاستبيان الخاص بهذه الدراسة، السؤال رقم 85.

من الشركات.[1] أما النسبة الباقية من الأفعال (10 في المائة) فقد أفادت الدول بأن محققي الشرطة يكتشفونها بشكل مباشر أو يحصلون عليها من تقارير مقدمي خدمة الإنترنت.

وتعتبر صورة الجريمة السيبرانية في نظر سلطات إنفاذ القانون، كأي جريمة، بالضرورة ناقصة لكَوْنها مُرَكّبة من امْتِزَاج قضايا فردية تم التحقيق فيها ومعلومات استخباراتية جنائية بشكل أوسع. وتثير طبيعة الجريمة السيبرانية عبر الحدود الوطنية تحديا – بوصول خيوط إجراءات التحقيق إلى الخوادم أو عناوين برتوكولات الإنترنت خارج البلاد – يولد تأخيرات، في حين تعتبر هناك ترابط بين آليات التعاون الرسمية أو غير الرسمية.

الشكل 5–1: مصادر بلاغات الجريمة السيبرانية إلى الشرطة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 78. (رقم=61)

وكما ذكرت إحدى الدول في أفريقيا، على سبيل المثال، بأن "أغلب الجرائم، بما فيها الجرائم التي لم يُبلغ عنها، تنطوي على أبعاد عابرة للحدود الوطنية، حيث تعتبر معظم الأهداف خارج نطاق الحدود الوطنية".[2] في حين أن دولة أخرى في أفريقيا أيضا، ذكرت أن *"أغلب الجرائم المبلغ عنها قد بدأت خارج هذه الدولة، حيث تعمل في معظم الحالات كمَمَر"*، بينما أوضحت دولة في أوروبا أن *"كل التحقيقات التي تم إجراؤها بشأن الجريمة السيبرانية في السنوات الخمس الماضية كانت ذات بعد عابر للحدود الوطنية. والأمثلة على ذلك جرائم ذات صلة باستخدام حسابات بريد إلكتروني، وشبكات تواصل اجتماعي، وخوادم فرعية"*.[3]

وبالإضافة إلى العناصر عبر الوطنية، فإن التقاعس عن عدم الإبلاغ عن أفعال الجريمة السيبرانية قد يسهم في المقام الأول في تضييق صورة هذه الظاهرة الرئيسية. وفي هذا الصدد؛ فإن نسبة 90 في المائة من أفعال الجريمة السيبرانية التي تصل إلى علم الشرطة من خلال إبلاغ الضحايا، فإن الدول–في هذا المقام–تقدر النسبة الواقعية لضحايا الجريمة السيبرانية التي تم إبلاغ الشرطة عنها تمثل تقريبا واحدا في المائة فقط.[4] هذا، وتظهر إحدى الدارسات التي اضطلع بإجرائها أحد كيانات القطاع الخاص، أن نسبة 80 في المائة من الضحايا الأفراد للأفعال الرئيسية التي تشكل الجريمة السيبرانية لا يبلغون الشرطة عن الجريمة.[5]

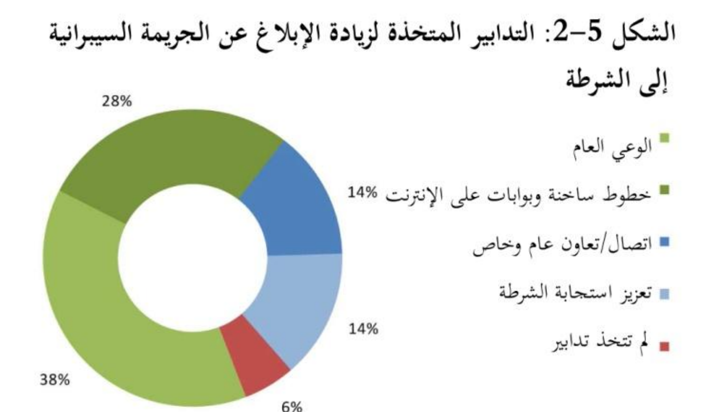
---

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 78.
[2] الاستبيان الخاص بهذه الدراسة، السؤال رقم 83
[3] المرجع السابق.
[4] الاستبيان الخاص بهذه الدراسة، السؤال رقم 82
[5] Symantec. 2012. *Norton Cybercrime Report 2012*.

وتعزي الدول المجيبة على الاستبيان تدني الإبلاغ عن أفعال الجريمة السيبرانية إلى عدد من العوامل، منها: انعدام ثقة العامة في قدرة الشرطة على التصدي للجريمة السيبرانية، عدم الوعي بالإيذاء وآليات الإبلاغ، علاوة على شعور الضحايا بالخجل والارتباك، وإلى تخوُّف الشركات من المخاطر المتصورة التي قد تهدد سمعتها. وقد ذكرت إحدى الدول، على سبيل المثال، أن: *"مسألة وضع تقديرات تعتبر من الأمور البالغة الصعوبة. فالبنوك والشركات تنأى بنفسها من الإبلاغ عن الجريمة السيبرانية نظرا للمخاطر التي قد تنال من سمعتيهما"*.[1] إلى جانب ذلك، أوضحت دول أخرى أن: *"معظم الضحايا لا يدركون حتى أنهم أصبحوا أهدافا، أو أن الأضرار التي لحقت بهم تعتبر غير ذات أهمية بما فيه الكفاية لهم، ولذلك لا يعيروها أي اهتمام"*.[2] وعندما تصل الحالات إلى علم الشرطة، فإن التحقيق عقب الواقعة يكشف عن مجموعة من الضحايا والجناة أوسع بكثير مما تم تحديده أساسا مع بداية إحدى الحالات. وقد ذكرت إحدى الدول المجيبة أن "بعضا من هذه [الجرائم] قد تكون أكثر شيوعا [من تلك التي تم الإبلاغ عنها].[3]

وأفادت العديد من الدول المجيبة بأن هناك استراتيجيات ونُهُجا مستخدمة لزيادة الإبلاغ عن الجريمة السيبرانية. وكما هو موضح في الشكل 5-2؛ فإن من هذه الاستراتيجيات والنُهُج المستخدمة: استخدام حملات التوعية العامة، إنشاء نظم للإبلاغ عبر الإنترنت وإتاحة خطوط ساخنة لذلك الغرض، الاتّصال بين كيانات القطاع الخاص، وأخيرا تعزيز التوعية الشرطية وتبادل المعلومات. هذا، وقد أفادت نسبة 10 في المائة من أصل 60 في المائة من الدول المجيبة على الاستبيان الملحق بهذه الدراسة، بأنها لم تضطلع باتخاذ أية تدابير تهدف إلى زيادة الإبلاغ عن أفعال الجريمة السيبرانية.[4]

الشكل 5-2: التدابير المتخذة لزيادة الإبلاغ عن الجريمة السيبرانية إلى الشرطة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 79. (رقم=75، 107)

وأظهرت أيضا ردود الدول الحاجة إلى أن تعمل سلطات إنفاذ القانون بشكل مباشر مع الجهات الفاعلة الأخرى، مثل القطاع الخاص، وذلك بغية زيادة الإبلاغ عن الجريمة السيبرانية علاوة على الأغراض الاستخباراتية. فعلى سبيل المثال، أوضحت إحدى الدول أنه من الأهمية بمكان "التواصل على

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 82.
[2] المرجع السابق.
[3] الاستبيان الخاص بهذه الدراسة، السؤال رقم 82.
[4] الاستبيان الخاص بهذه الدراسة، السؤال رقم 79

مدار الـ24 ساعة بين الإداريين القائمين على إدارة أحد المواقع الإلكترونية الهامة ومقدمي خدمة الإنترنت وأجهزة الشرطة، بالإضافة إلى مركز لتنسيق المجريات الأمنية". وأيضا، أفادت دولة أخرى من إحدى دول الأمريكتين بأن *"الشرطة الاتحادية تسعى لإبرام اتفاقيات مع الشركات العامة والخاصة بحيث يتم إبلاغ الشرطة الاتحادية إلكترونيا عن الجرائم المرتكبة ضد أي من هذه الشركات أو عملائها"*.[1] مع ذلك، وبشكل عام، فإن نسبة البلاغات المقدمة بشأن أفعال الجريمة السيبرانية من الشركات الضحايا أو مقدمي خدمة الإنترنت تعتبر نسبة منخفضة بشكل نسبي، مما يوحي بضرورة التوعية الإضافية وتطوير الشراكات بين القطاعين العام والخاص، وذلك من أجل تعزيز عمليات الإبلاغ عن أفعال الجريمة السيبرانية من هذه المصادر. بيد أن تكوين الشراكات بين القطاعين العام والخاص ومسؤوليات مقدمي خدمة الإنترنت قد تناولها الفصل الثامن بمزيد من التفصيل (المنع). أما التفاعلات بين سلطات إنفاذ القانون ومقدمي الخدمات الآخرين أثناء تحقيقات الشرطة قد تم تناولها أدناه في هذا الفصل.

من الواضح أن السمة البارزة في الشكل 5-1 تتمثل في انخفاض نسبة أفعال الجريمة السيبرانية التي يتم الكشف عنها من قبل المحققين المكلفين بإنفاذ القانون في ضوء غياب بلاغات الضحايا. ووفقا لذلك؛ لم تشر الدول المجيبة بشكل عام - في ردودها الخطية على الاستبيان - إلى إجراء أية تحقيقات استباقية. ومع ذلك، فإحدى الدول قد لاحظت أن "بعض قضايا أفعال الجريمة السيبرانية تصل إلى علم أجهزة الشرطة أثناء أداء الأخيرة لأنشطتها المهنية"[2]. وفي هذا الصدد أيضا، أفادت إحدى الدول الأوروبية أن "التحقيقات تبدأ غالبا في جرائم استغلال الأطفال في المواد الإباحية من المعلومات التي ترد من إحدى هيئات الشرطة الأخرى، والمصادر المفتوحة"، مما يشير إلى الأعمال الاستخباراتية الضِمْنِيّة التي تضطلع بها الشرطة.

ويعتبر توزيع مصدر الأفعال التي تشكل الجريمة السيبرانية المحددة ذا دلالة، بشكل جزئي، للتحديات المتمثلة في التصدي لكل من الأهداف الاستراتيجية والتكتيكية لحفظ الأمن والنظام العام. حيث تعتبر الأهداف الاستراتيجية لحفظ الأمن والنظام العام بمثابة تهديد مُوَجّه ويتعلق بأهداف سلطات إنفاذ القانون على المدى الطويل، مع التركيز على ملابسات الجرائم الجسيمة وأسبابها الجذرية. إلى جانب ذلك، تعتبر الأهداف التكتيكية لحفظ الأمن والنظام العام بمثابة وَقَائِع مُوَجّهة وفي وقت حَرِج، مع التأكيد على الحفاظ على الأدلة وخيوط التحقيق التالية، حيث يعتبر، في حالة الجريمة السيبرانية؛ اسْتِغْلاَل وقت الشرطة والموارد الضرورية للتعامل مع القضايا الفردية من الأمور الجوهرية. وكما تمت مناقشته لاحقا في هذا الفصل؛ فقد سلطت العديد من الدول الضوء على الكميات الهائلة من الأدلة المرتبطة بالتحقيقات في الجريمة السيبرانية، وطبيعة الوقت المستغرق في التحقيقات بشأن الحالات المبلغ عنها. فعلى سبيل المثال، ذكرت إحدى دول الأمريكتين، بأنه "قد زادت الطبيعة المعقدة للجريمة السيبرانية، وأركان الجريمة السيبرانية كجرائم تقليدية، مما يضع متطلبات إضافية تتمثل في التدريب ورِعَايَة المحققين ذوي المهارات العالية، والخبراء التقنيين، وأيضا زيادة الفترات الزمنية التي تحتاجها مجريات التحقيق

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 79.

[2] الاستبيان الخاص بهذه الدراسة، السؤال رقم 78.

في القضايا الفردية".[1] وعند هذا المنحى، فإن قدرة هيئات إنفاذ القانون في العديد من الدول مكرسة بشكل كامل لاستعراض الحالات اليومية. وفي مستعرض الرد على تساؤل بشأن قدرة السلطات المعنية بإنفاذ القانون على الاضطلاع بإجراءات تحقيقات الطب الشرعي، فعلى سبيل المثال، أفادت إحدى الدول الأفريقية ردا على هذا التساؤل بأن "المتاح من محققي/ مُسْتَجْوِبِي الطب الشرعي على المستوى الفيدرالي يعتبر عددا قليلا، ولكن ليس بما يكفي لخدمة الدولة بأكملها"، حيث يوجد مختبر فني واحد فقط.[2] كما أوضحت دولة أخرى من إحدى دول الأمريكتين بأن "التحدي لا يتجسد في الخِبْرَة، إنما يكمن في كمية البيانات التي يجب تحليلها".[3] وقد تم تناول طبيعة التحقيقات القضائية وقدرة هيئات إنفاذ القانون في هذا المجال بمزيد من التفصيل في الفصل السادس (الأدلة الإلكترونية والعدالة الجنائية).

بالإضافة إلى التحديات التي تحوم حول القدرات والموارد، فإن نطاق التحقيقات الاستباقية المعنية بالجريمة السيبرانية التي يمكن أن تجريها هيئات إنفاذ القانون، قد تتأثر أيضا بالاختلافات الجوهرية بين نظم القانون العام والقانون المدني فيما يتعلق بالرقابة القضائية وجهاز النيابة العامة على المراحل الأولية من التحقيق،[4] فضلا عن ماهية نطاق إجراءات التحقيق التدخلية التي يُسمح بها في التحقيقات القائمة على المعلومات الاستخباراتية أو التحقيقات المرْتَقَبة لمثل هذه المعلومات. وعلى النحو الذي تم تناوله في هذا الفصل، فإن التحقيقات المعنية بالجريمة السيبرانية غالبا ما تستخدم أساليب لخدمة التحقيق، منها اعتراض الاتصالات والمراقبة الإلكترونية، والتي من شأنها أن تنتهك الحقوق القائمة على الخصوصية. ومن ناحية أخرى، فإن التزامات الدول المعقودة بموجب القانون الدولي لحقوق الإنسان بحاجة إلى ضمان التوازن النسبي بين حماية الخصوصية والانتهاكات للأغراض المشروعة المراد بها منع الجريمة ومكافحتها. ويتناول القسم أدناه المعني بالخصوصية والتحقيقات هذا المجال بشكل مُفَصّل.

وبالرغم من ذلك، فإن سلطات إنفاذ القانون في الدول المتقدمة، وعددا منها في الدول النامية أيضا قد شاركت في تحقيقات متوسطة الأجل وطويلة الأجل. وغالبا ما تتشكل هذه الهيئات مِن وحدات سرية تستهدف المجرمين على مواقع التواصل الاجتماعي وغرف المحادثة والرسائل الفورية وخدمات النظراء (P2P). ومن الأمثلة على ذلك، اختراق منتديات "قرصنة بطاقات الائتمان"[5] عبر الإنترنت أو العثور عليها، واستخدام البحث الجنائي لفحص المنتديات التي يستخدمها الجناة في استغلال الأطفال في المواد الإباحية،[6] وتنكر الموظفين المكلفين بإنفاذ

---

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 84.

[2] الاستبيان الخاص بهذه الدراسة، السؤال رقم 110.

[3] المرجع السابق.

[4] أنظر على سبيل المثال، الشبكة الدولية لتعزيز سيادة القانون 2012، دليل الممارس: تقاليد القانون العام والقانون المدني

[5] See http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 and http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown

[6] See https://www.europol.europa.eu/sites/default/files/publications/2csefactsheet2012_0.pdf

القانون كقُصّر عبر الإنترنت،[1] وفحص خوادم القيادة والسيطرة للبرمجيات الخبيثة.[2] وجدير بالذكر، أن هذه التحقيقيات تتضمن مشاركة هيئات إنفاذ قانون متعددة، ومجموعة واسعة من إجراءات التحقيق، منها تلك التي تُنفذ بناء على أوامر من السلطة القضائية، مثل أوامر البحث والاعتراض. وفي الواقع، يتطلب كل من التحقيقات الاستراتيجية والتكتيكة الوصول إلى مجموعة من الصلاحيات التحقيقية – طبقا لمبادئ سيادة القانون – وفقا لأساس متأصل في سلطة قانونية. هذا ويتناول القسم التالي من هذا الفصل صلاحيات التحقيق في الجريمة السيبرانية الواردة في الصكوك الدولية والإقليمية، علاوة على القوانين الوطنية.

2-5 استعراض عام لصلاحيات التحقيق

الاستنتاجات الرئيسية:

- ترى العديد من الدول غير الأوروبية أن أطرها القانونية الوطنية غير كافية للتحقيق في الجريمة السيبرانية
- عموما، تظهر النُهج الوطنية لصلاحيات التحقيق في الجريمة السيبرانية، قواسم مشتركة أساسية أقل من تلك الخاصة بالتجريم
- بينما تختلف النُهج القانونية، فإن صلاحيات التحقيق تتطلب أن تشتمل هذه النُهُج على التفتيش والمصادرة، وأوامر قضائية للحصول على البيانات الحاسوبية، وماهية الوقت الحقيقي الذي تم استغراقه لجمع البيانات، والتحفظ على البيانات
- عَبْر العشرات من إجراءات التحقيق، أبلغت الدول في أكثر الأحيان عن وجود صلاحيات عامة (غير خاصة بالمجال السيبراني) في كل مستويات التحريات، أبلغ عدد من البلدان أيضا عن تشريعات خاصة بالمجال السيبراني، ولا سيما لضمان التعجيل في حفظ البيانات الحاسوبية والحصول على بيانات المشتركين المخزنة
- أبلغت دول عديدة عن عدم وجود صلاحيات قانونية لاتخاذ إجراءات متقدّمة، مثل التحاليل الجنائية الحاسوبية عن بُعد

الجرائم الخاصة بالسيبرانية والصلاحيات العامة للتحقيق

من المعروف أن كل المواد الإثباتية تتخذ الشكل الإلكتروني أو الرقمي، وتكون مخزّنة أو عابرة، وقد تتخذ شكل ملفات حاسوبية أو مواد منقولة أو سجلات أو بيانات فوقية أو بيانات شبكية. فالحصول على هذه الأدلة يتطلب مزيجا من التقنيات التقليدية وتقنيات جديدة لحفظ الأمن والنظام العام. وفي هذا الصدد، يجوز لسلطات

[1] See http://cdrc.jhpolice.gov.in/cyber-crime/

[2] http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Kuzmin,%20Nikita%20Complaint.pdf

إنفاذ القانون أن تستعير عمل الشرطة "التقليدي" (عقد لقاءات مع الضحايا، المراقبة البصرية السرية للمشتبه بهم) في بعض مراحل التحقيق، بيد أن النهج المتعلقة بالحاسوب تتطلب أجزاء أخرى من ذلك العمل التقليدي، حيث يمكن أن تشتمل على المراقبة والمصادرة، أو نسخ البيانات الحاسوبية من الأجهزة التي تخص المشتبه بهم، كما يمكن أن تتضمن الحصول على بيانات حاسوبية من أطراف أخرى مثل مقدمي خدمة الإنترنت، واعتراض المراسلات الإلكترونية، إذا اقتضى الأمر ذلك.

وفي حين يمكن تنفيذ بعض إجراءات التحقيق بواسطة الصلاحيات التقليدية، فإنه يصعب تكييف العديد من القواعد الإجرائية التي تستند إلى نهج يقوم على توجّهه في الحيّز المكاني للأشياء لجعلها تستند إلى نهج يشمل تخزين البيانات الإلكترونية وتدفّق البيانات في الوقت الحقيقي. وفي بعض الدول؛ يمكن الحصول على البيانات الحاسوبية من خلال الصلاحيات "التقليدية" المتمثلة في البحث والمصادرة "لأي شيء" يُعتقد أن له صلة بإحدى الجرائم، كما يساهم وجود قوانين معنية "بالتنصت" و"اعتراض الاتصالات" أيضا في توفير ما يكفي من الصلاحيات لبعض الجوانب المتعلقة بالتحقيقات في الجريمة السيبرانية. ومع ذلك، لا تعتبر القوانين الإجرائية التقليدية –في دول أخرى– مُؤَهّلة للتفسير لتستوعب البيانات غير المادية أو الاتصالات القائمة على برتوكولات الإنترنت. بالإضافة إلى ذلك؛ يجب أن تتمتع صلاحيات التحقيق بالقدرة على التصدي للتحديات، مثل طبيعة الأدلة الإلكترونية التي تتسم بسهولة زوالها وتغيّرها، واستخدام الجناة لتقنيات التشويش، بما في ذلك استعمال التشفير ووحدات الخدمة النائبة، وخدمة الحوسبة السحابية، ونظم الحاسوب "النَظِيفة" المصابة ببرمجيات خبيثة، ووصلات الإنترنت متعددة الموجه، (أو برامج إخفاء الهوية).[1] هذا، وتشكل هذه النّواحي، بشكل خاص، تحديات خاصة تعترض طريق الصلاحيات التقليدية. وفي هذا الشأن، أفاد العديد من الدول المجيبة على الاستبيان الخاص بالدراسة بأن صلاحيات التحقيق تعتبر فِي أَغْلَب الْأَوْقَات *"لا تتماشى مع التكنولوجيات الجديدة والناشئة"، كما أن "التشريعات [تعتبر] مُخَصّصة لتتلاءم مع البحث والتفتيش المادي، ولذلك فإن تعليمات القانون لا تشبع المتطلبات والمصالح والإجراءات الدستورية ذات الصلة بالتحقيقات في الجريمة السيبرانية"*.[2]

وفي ضوء ما تقدم، فإن الأطر القانونية للتحقيق في الجريمة السيبرانية – ما إذا كانت بالدرجة الأولى قوانين "عامة" أو "خاصة بالمجال السيبراني" – تتطلب كلا من: (1) نطاقا واضحا لتطبيق الصلاحية الممنوحة بغية ضمان اليقين القانوني في استخدامها؛ و(2) سلطة قانونية كافية للاضطلاع باتخاذ الإجراءات مثل ضمان التحفظ على البيانات الحاسوبية، والوقت الحقيقي لجمع البيانات المخزنة. وفي هذا الصدد، تمنح الأطر الإجرائية المتخصصة إمكانية تحديد المفاهيم ذات الصلة بشكل واضح، مثل: "البيانات الحاسوبية" في المقام الأول، فضلا

---

[1] See, for example, Feigenbaum *et al.*, 2007. A Model of Onion Routing with Provable Anonymity. *Financial Cryptography and Data Security Lecture Notes in Computer Science*, 4886:57-71; and Schwerha, J.J., 2010. *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers,"* Council of Europe Discussion paper, pp.9-10; Walden, I., 2013. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. *Privacy and Security for Cloud Computing. Computer Communications and Networks 2013*, pp.45-71.

[2] الاستبيان الخاص بهذه الدراسة، السؤال رقم 53.

عن البيانات "الباقية" والبيانات "العابرة".[1] كما أن هذه الأطر الإجرائية المتخصصة تسمح أيضا بالتَمْيِيز بين أنواع البيانات؛ مثل بيانات "المشترك" (تفاصيل التسجيل الأساسية لمستخدمي خدمة الحاسوب، مثل الاسم والعنوان) و "حركة مرور" البيانات (البيانات التي تشير إلى المنشأ، المقصد، المسار، الوقت، التاريخ، الحجم، المدة الزمنية، أو أي نوع من الاتصالات تمت من خلال أحد النظم الحاسوبية)، وأخيرا بيانات "المحتوى" (المحتوى الحقيقي لأي من الاتصالات).[2]

وقد سُئلت الدول، أثناء جمع المعلومات الخاصة بهذه الدراسة، عن وجود إما صلاحيات قانونية عامة أو خاصة بالفضاء السيبراني لعشرة إجراءات مختلفة ذات الصلة بالتحقيقات التي تضطلع بها سلطات إنفاذ القانون في الجريمة السيبرانية (والجرائم الأخرى التي تنطوي على أدلة إلكترونية). وتمثلت الإجراءات التحقيقية التي سُئلت الدول بشأنها في: (1) البحث الذي تضطلع به سلطات إنفاذ القانون عن البيانات الحاسوبية أو أجهزة الحاسوب، (2) مصادرة البيانات الحاسوبية أو أجهزة الحاسوب، (3) الأمر الصادر لأي شخص من الأشخاص لإمداد سلطات إنفاذ القانون بمعلومات عن أحد المشتركين، (4) الأمر الصادر لأي شخص من الأشخاص لإمداد سلطات إنفاذ القانون بحركة البيانات المخزنة، (5) الأمر الصادر لأي شخص من الأشخاص لإمداد سلطات إنفاذ القانون بمحتوى البيانات المخزنة، (6) الوقت الحقيقي المستغرق لجمع حركة البيانات، (7) الوقت الحقيقي المستغرق لجمع محتوى البيانات، (8) الأمر الصادر لأي شخص من الأشخاص بالحفاظ على سلامة البيانات الحاسوبية وصيانتها ووضعها تحت سَيْطَرَتِهم لفترة زمنية محددة ("الأمر المعجل بالتحفظ على البيانات)، (9) استخدام التحاليل الجنائية الحاسوبية عن بُعد، (10) وصول سلطات إنفاذ القانون المباشر للبيانات الحاسوبية خارج حدود الدولة (وصول للبيانات الحاسوبية "عبر الحدود").[3]

الشكل 5-3: النهج الوطنية للإجراءات التحقيقية في الجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 42-51. (رقم=55)

---

[1] Walden, I., 2003. Addressing the Data Problem. *Information Security Technical Report*, 8(2); Nieman, A., 2009. Cyberforensics: Bridging the Law/Technology Divide. *JILT,* 2009(1).

[2] Sieber, U., 2008. Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. *In*: Delmas-Marty, M., Pieth, M., Sieber, U. (eds.). *Les chemins de l'HarmonisationPénale/Harmonising Criminal Law*. Collection de L'UMR de Droit Comparé de Paris. Paris: Société de législation comparée.

[3] الاستبيان الخاص بهذه الدراسة، السؤال رقم 42-51.

ويقدم الشكل 5-3 لمحة عامة عن الأحكام القانونية القائمة التي تتناول الإجراءات العشرة الخاصة بالتحقيق، حسبما أفادت أكثر من 50 دولة من الدول المجيبة على الاستبيان الخاص بهذه الدراسة. وتبين الردود أن غالبية الدول تعول على الصلاحيات القانونية العامة الممنوحة للتحقيق في الجريمة السيبرانية. ويعتبر ذلك بمثابة الحالة المعمول بها في مجموعة من إجراءات التحقيق، والتي تشتمل على البحث والمصادرة والأوامر بشأن بيانات عناوين الأطراف الأخرى، الوقت الحقيقي المستغرق في جمع البيانات، وكذلك الأمر بالتحفظ المعجل على البيانات. ومن الملاحظ أن ما يقرب من نصف الدول المجيبة أشارت إلى أن إجراءات التحقيق التي تتسم بالتدخلية والتعقيد، مثل استخدام التحاليل الجنائية الحاسوبية عن بُعد، لم يقِرَّها القانون. بيد أن ما يقرب من نسبة 20 في المائة من الدول المجيبة، أفادت بأنه لا توجد صلاحية قانونية بشأن الوقت الحقيقي المستغرق في جمع البيانات الحاسوبية، أو تَنْظِيم التحفظ المعجل على البيانات الحاسوبية. علاوة على ذلك، أفادت نسبة 10 في المائة من الدول بأنه لا توجد صلاحية قانونية، حتى لأغراض البحث ومصادرة البيانات الحاسوبية وأجهزة الحاسوب.

وأخيرا، أظهرت الدول التي أفادت بوجود صلاحيات خاصة بالمجال السيبراني توزيعا جغرافيّا عَرِيضا في كافة أنحاء أوروبا وأمريكا الشمالية ومنطقة البحر الكاريبي، وجنوب شرق آسيا وغربها، وشمال وغرب أفريقيا. ومن الملاحظ أن غالبية إجراءات التحقيق تناولتها أحكام خاصة بالمجال السيبراني تمثلت في أوامر بالكشف عن بيانات المشترك، وقرارات للتحفظ المعجل على البيانات، هذا، وأفاد ما يقرب من 25 إلى 30 في المائة من الدول المجيبة بوجود أحكام خاصة بالمجال السيبراني تتناول هذه المجالات. وجدير بالذكر، أن الإجراءات المتعلقة بالبحث ومصادرة البيانات الحاسوبية وأجهزة الحاسوب تتناولها كل من الأحكام العامة والأحكام الخاصة بالمجال السيبراني، وتعتبر هذه إحدى الأمثلة التي ذكرها ما يقرب من نسبة 20 في المائة من الدول المجيبة.

كفاية صلاحيات التحقيق للجريمة السيبرانية

وفيما يتعلق بالكفاية المتوقعة لصلاحيات التحقيق، أظهرت الدول المجيبة على الاستبيان الخاص بهذه الدراسة نمطا مماثلا لقوانين التجريم، حيث أفاد ما يقرب من نسبة 70 في المائة من الدول الأوروبية المجيبة بكفاية صلاحيات التحقيق. بيد أن النسبة الباقية ارتأت أن صلاحيات التحقيق كافية "بشكل جزئي"، في حين اعتبرت دولة واحدة فقط من هذه النسبة الباقية بأن صلاحيات التحقيق غير كافية. وفي مناطق أخرى من العالم، أفاد ما بين نسبة 20 و65 في المائة من الدول المجيبة بأن صلاحيات التحقيق لا تعتبر كافية.

وعندما سئلت الدول عن ماهية الفجوات الرئيسية التي تعتري صلاحيات التحقيق، أشار العديد منها إلى عجز الصلاحية الممنوحة للدخول في الشبكات الإلكترونية بغية البحث عن المواد الثبوتية، فضلا عن عدم وجود صلاحية للتحفظ على البيانات الحاسوبية. كما أفادت دول أوروبية وأخرى من أوقيانوسيا بأن هناك حاجة *"لآلية للتحفظ المعجل على البيانات الحاسوبية لدعم صلاحيات البحث"*، بينما سلطت إحدى دول أمريكا الجنوبية الضوء على *"عدم وجود تنظيم للوصول إلى البيانات وسجلات الاتصال [فضلا عن] عدم وجود تنظيم لإمكانيات البحث الافتراضي"*.[1]

الشكل 5–4: كفاية القانون الوطني للتحقيقات في الجريمة السيبرانية

المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 53. (رقم=54)

ومن جهة أخرى؛ بينما أبلغت العديد من الدول بانعدام الإطار القانوني لتحديد ماهية الجريمة السيبرانية، فإن عددا قليلا من الدول الأخرى ذكرت أيضا نجاح توسيع نطاق الصلاحيات العامة. فعلى سبيل المثال؛ أفادت إحدى دول جنوب أفريقيا بأن *"قانون الإجراءات الجنائية يجيز للدولة مصادرة أي شيء ... [على الرغم من أن] القانون لم يأت على ذكر الجريمة السيبرانية بشكل خاص"*.[2] وأفادت بعض الدول أيضا بأن صلاحيات التحقيق ذات الصلة بالحاسوب والأجهزة الأخرى تعتبر بمثابة ممارسة جيدة "تسري على كافة الجرائم وليس فقط جرائم الحاسوب التقليدية"، وأن القوانين الإجرائية ذات الصلة ينبغي أن تكون *"شاملة"* و*"مُحْكَمة"*.[3]

وبشكل عام؛ توجد ثلاثة اتجاهات رئيسية تمخضت عن ردود الدول على الاستبيان الملحق بهذه الدراسة: فبعض الدول ليست لديها قوانين خاصة تتعلق بالتحقيقات في الجريمة السيبرانية، وتطبق الصلاحيات الإجرائية التقليدية بِمِقْدارِ ما تقْتَضَى أحد التفسيرات الواسعة. وعند منحى آخر، قد قامت دول أخرى بتعديل الصلاحيات العامة للتحقيق فيما يتعلق ببعض القضايا المحددة، وذلك من خلال استعمال صلاحيات عامة

---

[1] المرجع السابق.
[2] المرجع السابق
[3] المرجع السابق

وصلاحيات خاصة بالفضاء السيبراني مؤهلة للتطبيق على مجموعة من الإجراءات مثل الأوامر الخاصة بالبيانات، وأوامر البحث والمصادرة، بالإضافة إلى قرارات التحفظ على البيانات. وأخيرا؛ قد أدرجت عدد من الدول مجموعة شاملة من صلاحيات التحقيق الجديدة مخصصة بشكل محدّد للحصول على الأدلة الإلكترونية. وفي هذا الصدد على سبيل المثال؛ تحدد الأحكام التشريعية في إحدى دول جنوب أوروبا أربعة طرق مختلفة يمكن بموجبها اعتبار أن البيانات "*مصادرة*" – (1) مصادرة الوسيط (المستخدم) نفسه؛ (2) عمل نسخة؛ (3) الحفاظ على سلامة البيانات بدون إزالة أو نسخ، و(4) إزالة البيانات أو حجب الوصول إلى البيانات. وتساعد مثل هذه الأحكام في التخلص من عدم اليقين القانوني المحيط بتطبيق صلاحيات التحقيق "التقليدية".

الصلاحيات الشاملة للتحقيق في الجريمة السيبرانية: مثال وطني من دولة في جنوب

مصادرة البيانات الحاسوبية

مصادرة البيانات الحاسوبية، اعتمادا على ما يعتبر الأكثر تناسبا أو غير متناسب، مع الأخذ في الاعتبار مصالح الحالة والتي قد تأخذ الأشكال التالية:

أ) مصادرة أدَوات دعم النظام الحاسوبي، أو متوسط البيانات الحاسوبية المخزنة، علاوة على الأجهزة المطلوبة لقراءة البيانات؛

ب) عمل نسخة من هذه البيانات الحاسوبية في أحد وسائل الدعم المستقلة والتي ينبغي إرفاقها مع الملف؛

ج) المحافظة على سلامة البيانات الحاسوبية باستعمال الوسائل التكنولوجية، وذلك بدون نسخ البيانات أو إزالتها؛

د) إزالة البيانات الحاسوبية أو حجب الدخول أيضا.

يظهر تتبع العلاقة بين الصلاحيات التشريعية المتخصصة القائمة والاكْتِفَاء المتصور لأطر التحقيق في الجريمة السيبرانية، قدرا من الملاءمة للدول التي أجابت على الاستبيان الخاص بهذه الدراسة. وفيما يتعلق بالدول التي أفادت بأن أطر التحقيق تعتبر "كافية" أو "كافية بشكل جزئي"؛ فإن ما يقرب من نسبة 40 في المائة من كل إجراءات التحقيق التي سئلت بشأنها الدول قد تناولتها صلاحيات خاصة بالمجال السيبراني. وعلى النقيض من ذلك، فإن الدول التي أفادت بعدم كفاية أطر التحقيق، فإن نسبة 20 في المائة فقط من كل إجراءات التحقيق قد تناولتها صلاحيات خاصة بالفضاء السيراني.[1] وتبرز هذه النَتِيجَة أهمية تطوير صلاحيات التحقيق المتخصصة، كحد أدنى، في حالة إذا تطرق الشك في نطاق الصلاحيات التقليدية. ويوضح الفصل السابع (التعاون الدولي) من هذه الدراسة أن الطبيعة العالمية للجريمة السيبراني تعني أن الافتقار إلى صلاحيات التحقيق في إحدى الدول يمكن أن يكون لديه تأثير على دول أخرى إذا طلبت الأخيرة التعاون الدولي في جمع الأدلة خارج الحدود الوطنية.

وكما تم مناقشته في الفصل الثالث (الأطر والتشريعات)، فإن عددا من الصكوك الدولية والإقليمية توفر أطرا شاملة لصلاحية التحقيق.[2] هذا، ويوجز الجدول الوارد في الملحق الثالث ماهية الصلاحيات – كل بند على

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 42-51، والسؤال رقم 53.

[2] أنظر الفصل الثالث (التشريعات والأطر) القسم 3-1 مقدمة-دور القانون، تصنيفات القانون ذات الصلة.

حدة – في عدد من هذه الأطر. ويستمر القسم التالي من هذا الفصل في تناول، بالتفصيل، طبيعة الأحكام المعنية بصلاحيات التحقيق، الواردة في كل من الصكوك متعددة الأطراف وعلى النحو المذكور من الدول على المستوى الوطني من خلال الاستبيان المرافق لهذه الدراسة، وذلك للحصول على صلاحيات لإجراءات تتعلق: بـ (1) التفتيش والمصادرة، (2) حِفْظ البيانات الحاسوبية، (3) الأوامر المتعلقة بالبيانات الحاسوبية، (4) الوقت الحقيقي المستغرق لجمع البيانات الحاسوبية، (5) استخدام أدوات التحليل الجنائي عن بُعد، و(6) الوصول المباشر لسلطات إنفاذ القانون إلى البيانات خارج الحدود الوطنية.

التفتيش والمصادرة

كما ذُكر أعلاه؛ فإن العديد من الدول قد تواجه مجموعة من التحديات عند توسيع نطاق البحث والمصادرة "التقليدية" للبيانات غير المادية.[1] ولهذه الأسباب؛ تتضمن سبعة من الصكوك[2] الدولية أو الإقليمية المعنية بمكافحة الجريمة السيبرانية أحكاما منوط بها تحديد الصلاحيات الخاصة بتفتيش نظم الحاسوب أو وسائط تخزين البيانات الحاسوبية، أو الوصول إليها بشكل مماثل. وجدير بالذكر أن ستة من هذه الصكوك توفر أيضا تمهيدا لنطاق البحث لنظام حاسوبي آخر داخل إقليم

أوامر التفتيش والمصادرة: مثال وطني من دول الأمريكتين

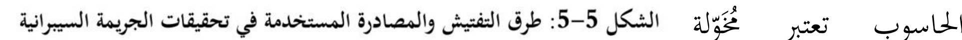
(2) أي أمر يصدر بموجب هذه المادة، يخَوّل لأي من ضباط الشرطة صلاحية:
(أ) مصادرة أي حاسوب، بيانات، برامج، معلومات، وثائق أو أي شيء يعتقد معه ضابط الشرطة بشكل مناسب بأنه دليل على ارتكاب جريمة أو على وشك ارتكاب جريمة وفقا لهذا القانون؛
(ب) فحص تشغيل، أو التحقق من تشغيل أي حاسوب وفقا للمشار إليه في الفقرة (أ)؛
(ج) استخدام أو ما يدعو إلى استخدام أي حاسوب وفقا للمشار إليه في الفقرة (أ) للتفتيش عن أية برامج أو بيانات موجودة في جهاز الحاسوب أو متاحة؛
(د) الوصول إلى أي من المعلومات، رمزا أو تكنولوجيا والتي من شأنها أن تكون لديها قدرة نقل أو تحويل أحد البرامج أو البيانات المشفّرة – الموجودة في جهاز الحاسوب أو متاحة – إلى شكل أو نصوص قابلة للقراءة ومَفْهُومة، وذلك لأغراض التحقيق في أي جريمة وفقا لهذا القانون؛
(هـ) تحويل أحد البرامج أو البيانات المشفّرة الموجودة في جهاز حاسوب آخر وارد بشكل محدد في أمر التفتيش والمصادرة، في حالة إذا كانت هناك أسباب مناسبة للاعتقاد بأن البيانات الحاسوبية ذات العلاقة بارتكاب الجريمة قد تكون مخزنة في ذلك النظام الحاسوبي الآخر؛
(و) عمل نسخة من أي برامج أو بيانات موجودة في الحاسوب، مع الحفاظ عليها، المشار إليه في الفقرة (أ) أو الفقرة (هـ)، وأي برامج أو بيانات أخرى موجودة في الحاسوب.

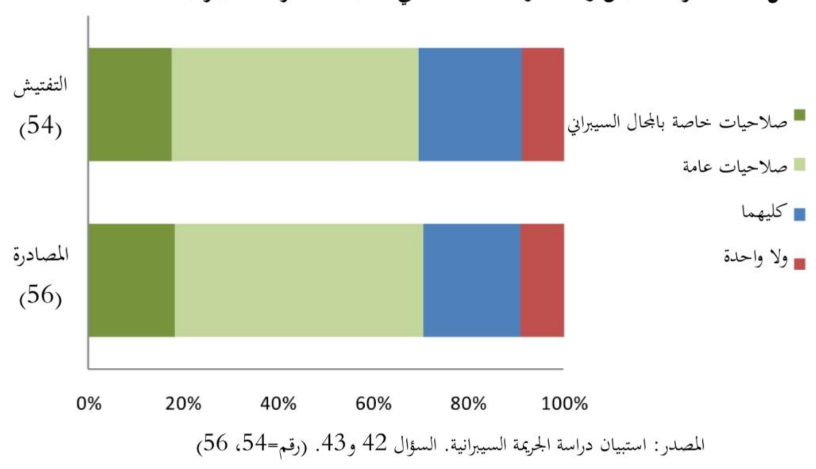
[1] See, for instance, Brenner, S. W., Frederiksen, B.A., 2002. Computer Searches and Seizures: Some Unresolved Issues. *Mich. Telecomm. Tech. L. Rev.* 39(8); Kerr, O.S., 2005. Search Warrants in an Era of Digital Evidence. *Mississippi Law Journal*, 75:85.

[2] مشروع اتفاقية الاتحاد الأفريقي، المواد 3-50، 3-51؛ مشروع القانون النموذجي للسوق المشتركة لشرق افريقيا والجنوب الأفريقي المواد 37، 33؛ القانون النموذجي لدول اتحاد الكومنولث المادتان 12، و14؛ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 19، المشروع التوجيهي للجماعات الاقتصادية لدول غرب أفريقيا، المادة 33، مشروع النصوص التشريعية للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 20، الاتفاقية العربية بشأن مكافحة جرائم المعلومات المواد 26، 27

الدولة، في حالة إذا ثبت أن المعلومات المعنية غير موجودة في النظام الأصلي أو في الوسائط التي تم تفتيشها.[1] أيضا؛ تستجلي عددا من الصكوك متعددة الأطراف والطرائق التي يمكن بموجبها "مصادرة" البيانات الحاسوبية. فعلى سبيل المثال؛ ينص القانون النموذجي لدول اتحاد الكومنولث على أن مصطلح " مُصَادَر" يشتمل على "تناول نسخة مطبوعة من مخرجات البيانات الحاسوبية".

أظهرت الردود – على المستوى الوطني – على الاستبيان الملحق بهذه الدراسة أن أوامر تفتيش ومصادرة البيانات الحاسوبية وأجهزة الحاسوب تعتبر مُخَوّلة بموجب قوانين الإجراءات الجنائية العاملة لغالبية الدول (حوالي 50 في المائة)، بالأحرى من صلاحيات خاصة بالمجال السيبراني.[2] أما فيما يتعلق بتطبيق الصلاحيات العامة للتفتيش؛ أوضحت إحدى دول شرق آسيا أن الأحكام التقليدية بشأن أوامر التفتيش يمكن تطبيقها على "تفتيش الحاسوب"، بيد أن هذا الحكم مجاز فقط لتفتيش أجهزة الحاسوب ولا يسري على البيانات الحاسوبية.[3] كما أن الملاحظ في هذا الصدد، أن أقل من نسبة 20 في المائة من الدول المجيبة أشارت إلى وجود صلاحيات خاصة بالفضاء السيبراني تتعلق بالتفتيش والمصادرة.


الشكل 5-5: طرق التفتيش والمصادرة المستخدمة في تحقيقات الجريمة السيبرانية



وقد ذكرت فقط نسبة تقل عن 10 في المائة من الدول بأنه لا توجد أي صلاحية للتفتيش والمصادرة على الإطلاق، على الأقل للبيانات الحاسوبية. وعلى سبيل المثال؛ ذكرت إحدى دول غرب آسيا أنه "فيما يتعلق بالوصول إلى الأجهزة والأدَوات، فإن قانون الإجراءات الجنائية يتعامل مع حالات التفتيش المادي للمنازل من قِبَل أحد أعضاء الشرطة القضائية، ولكن لا يتصدى القانون الإجرائي للجريمة الإلكترونية". ومن جهة أخرى فإن النصوص لا تجيز لأعضاء الشرطة القضائية الدخول على الشبكات الإلكترونية والبريد الإلكتروني على أساس

---

[1] مشروع اتفاقية الاتحاد الأفريقي؛ مشروع القانون النموذجي للسوق المشتركة لشرق افريقيا والجنوب الأفريقي؛ القانون النموذجي لدول اتحاد الكومنولث؛ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية؛ مشروع النصوص التشريعية للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات؛ الاتفاقية العربية بشأن مكافحة جرائم المعلومات.

[2] الاستبيان الخاص بهذه الدراسة، السؤال رقم 42، و43

[3] المرجع السابق.

الاشتباه في ارتكاب جريمة".[1] هذا، وقد ذكرت أيضا هذه الدولة أن هناك حاجة لإصلاح قانوني بغية توفير صلاحيات، وحاليا *"إن هذا الدخول [قد] تم في عدم وجود أحد الأحكام القانونية، فإن ذلك يعني انتهاك أحكام الدستور والقانون"* .

التحفظ على البيانات الحاسوبية

من المعروف أن تخزين البيانات الحاسوبية يحتاج إلى موارد ومال، ونتيجة ذلك؛ تعتبر البيانات الحاسوبية إجْمالا مخزنة لفترة زمنية فقط والتي تعتبر في أمس الحاجة للمعالجة. ففي حالة محتوى "المحادثة النصية" أو "نقل الصوت باستخدام بروتوكول الإنترنت"، على سبيل المثال، التي تمر من خلال إحدى الخدمات التي يقدمها مزودو خدمة الإنترنت، قد تحتاج فقط فترة زمنية للأغراض التشغيلية، مثل تحديد عيوب النظام، أو إعداد فاتورة العميل. ويتراوح الوقت المستغرق لهذه العملية ما بين بضع ثوان إلى ساعات، أو بضع أيام أو أسابيع. بالإضافة إلى التكلفة الواقِعِيّة للنتائج المترتبة على تخزين البيانات، فإن لدى العديد من الدول أيضا أطر حماية البيانات التي تحدد أنه لا يجب الاحتفاظ بالبيانات لفترات زمنية أطول من تلك المطلوبة للأغراض التي تمت معالجة البيانات من أجلها.[2] ونظرا لمتطلبات الإجراءات القانونية، في الحالات العابرة للحدود الوطنية، أو طلبات التعاون الدولي، فإن ذلك قد يستغرق بشكل ميسر وقتا أطول من العمر الافتراضي للبيانات قبل أمر التفتيش ذات الصلة أو الحصول على أمر بتوريد البيانات المخزنة.[3]

الأمر المستعجل بالتحفظ على البيانات الحاسوبية: مثال وطني من دولة في جنوبي أفريقيا

أوامر التحفظ

(1) يجوز لأي سلطة تحقيق في حالة وجود أسباب مناسبة للاعتقاد بأن البيانات معرضة للفقد أو التعديل، أن تخاطب هيئة المحكمة المنعقدة غرفة المشورة لاستصدار أمر بالتحفظ المعجل على البيانات التي قد تم تخزينها أو معالجتها عن طريق أحد أنظمة الحاسوب، وكذلك التحفظ المعجل على أي من تقنيات المعلومات والاتصالات الأخرى.

(2) لأغراض المادة (1)، فإن البيانات تتضمن حركة البيانات ومعلومات المشترك .

(3) أي أمر يصدر بموجب المادة (1)، تعتبر سارية المفعول:

(أ) حتى الوقت الذي يستغرقه بشكل مناسب التحقيق في الجريمة؛

(ب) في حالة تحريك الدعوى الجنائية، حتى صدور حكم نهائي في القضية؛ أو

(ج) حتى الوقت الذي تعتبره هيئة المحكمة المنعقدة في غرفة المشورة مناسبا.

وبالتالي؛ تنطوي سبعة صكوك دولية وإقليمية على أحكام تهدف إلى تأسيس آليات هامة للتحقيقات في الجريمة السيبرانية

---

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 53

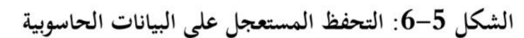
[2] أنظر الفصل الثامن (المنع)، القسم 8-3، مكافحة الجريمة السيبرانية، القطاع الخاص والأوساط الأكاديمية، مكافحة الجرائم السيبرانية من قبل مقدمي خدمات الإنترنت، ومقدمي خدمات الاستضافة.

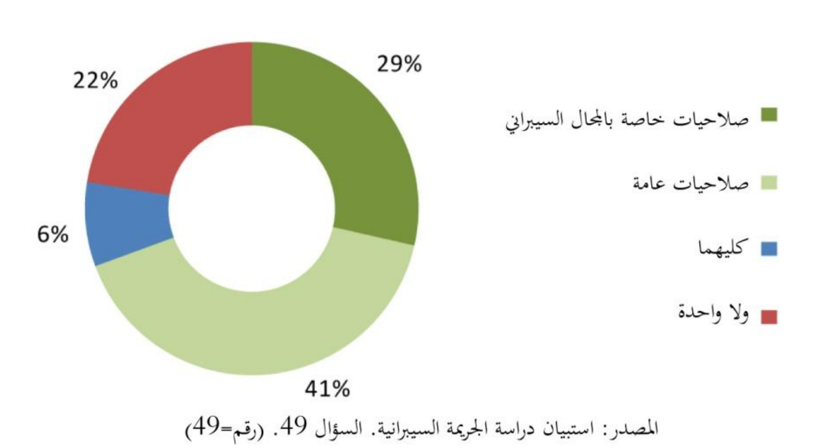
[3] James Tetteh, A.-N., Williams, P., 2008. *Digital forensics and the legal system: A dilemma of our times.* Available at: http://ro.ecu.edu.au/adf/41/

منوط بها منع حذف البيانات الحاسوبية.[1] فهذه الإجراءات يمكن أن تمنح تأثيرا بإعطاء أمر لأي شخص يتحَكّم في البيانات الحاسوبية بأن يحافظ ويصون سلامة البيانات لفترة زمنية محددة، أو خلافا لذلك، الاضطلاع بإجراءات سريعة لتأمين البيانات، وذلك من خلال أحد أوامر التفتيش والمصادرة. هذا، وقد تشتمل المواصفات الرئيسية للأحكام المعنية بالتحفظ "المعجل" تطبيق مجموعة من الشروط والضمانات أكثر محدودية من الكشف عن البيانات، ويرجع ذلك إلى كونها أقل عرضة من الطبيعة المجْحِفة لإجراءات التحفظ. ويجب مع ذلك ملاحظة أن الآليات الدولية لحقوق الإنسان قد قضت بأن مجرد تخزين كميات من المعلومات الفردية يعتبر في هذا الصدد أحد أشكال التدخل في الحق في الحياة الخاصة.[2] ولذلك؛ لازال يتطلب إصدار أوامر التحفظ تقييما لمدى تَنَاسُب هذا الإجراء، ولاسيما إذا تطلب الامتثال إلى الأمر الصادر بيانات محددة للاحتفاظ بها لمدة أطول من الفترة الزمنية المتوخاة من قِبَل التشريعات المعنية بحماية البيانات.

وبالرغم من ذلك، فإن التحفظ على البيانات يعتبر إجراءً هاما يتمثل في الحفاظ على الأدلة الجوهرية قبل أمر الكشف الكامل، وبخاصة في سياق التحقيقات عبر الحدود الوطنية. بيد أنه في الواقع، يعتبر الفصل بين الالتزامين المعنيين "بالتحفظ على البيانات" و"الكشف عن البيانات" ذا دلالة أساسية في الإجراء المتخذ[3].

وأخيرا – على الصعيد الوطني – يعتبر الأمر بالتحفظ المعجل على البيانات بمثابة الإجراءات التي تحظى بنسبة عالية بين الدول التي ذكرت أنه يشكل أحد الصلاحيات الخاصة في المجال السيبراني، وذلك ربما يرجع لتأثير الصكوك الدولية والإقليمية المعنية بمكافحة الجريمة السيبرانية. وبالرغم من ذلك؛ فقد أشارت الدول المجيبة أيضا إلى أن الأحكام العامة يمكنها أن تتناول الإجراء بطرق مختلفة. فعلى سبيل المثال؛ ذكرت إحدى دول غرب آسيا أن الأحكام المعنية


الشكل 5–6: التحفظ المستعجل على البيانات الحاسوبية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 49. (رقم=49)

---

[1] مشروع اتفاقية الاتحاد الأفريقي، المواد 3–53، مشروع القانون النموذجي للسوق المشتركة لشرق افريقيا والجنوب الأفريقي المواد 33–35؛ القانون النموذجي لدول اتحاد الكومنولث المادة 17؛ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 16، المشروع التوجيهي للجماعات الاقتصادية لدول غرب أفريقيا، المادة 33، مشروع النصوص التشريعية للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 23، الاتفاقية العربية بشأن مكافحة جرائم المعلومات المواد 23.

[2] أنظر على سبيل المثال، المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 81/9248.

[3] See Brown, I., 2010. Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, 19(2):107.

بالتفتيش والمصادرة قد فُسّرَت على أنها تنص على الأمر بالتحفظ المعجل. وفي هذا السياق، أوضحت أيضا إحدى دول الجنوب الأفريقي بأنه يمكن التحفظ على البيانات الحاسوبية طبقا لتشريعاتها من خلال مصادرة الحاسوب، في حين أن إحدى دول غرب أوروبا أفادت بأنها تستخدم الأحكام العامة المعنية بمصادرة المراسلات والمعلومات الأخرى.[1] وإضافة إلى ذلك؛ فقد أشار، من ناحية أخرى، أكثر من نسبة 20 في المائة من الدول المجيبة على الاستبيان الخاص بهذه الدراسة أن القانون الوطني لا يتضمن صلاحية لضمان التحفظ المعجل على البيانات. وغني عن البيان؛ أن عدم وجود سلطة قانونية لمثل هذه الأداة الهامة للتحقيق تمثل تحديا كبيرا، ليس فقط لتلك الدول المعنية، إنما أيضا لأي دولة من الدول الأخرى التي تسعى لطلب المساعدة في التحقيق.

الأوامر الخاصة بالبيانات الحاسوبية

وعلى النحو الذي نُوقش في الفصل الأول (الموصولية والجريمة السيبرانية)، فإن القطاع الخاص يملك ويسَيّر جزءا كبيرا من البنية التحتية ونظم الحاسوب المستخدمة لاتصالات الإنترنت. ولذلك يسيطر مقدمو خدمة الإنترنت، فضلا عن مقدمي الاتصالات الإلكترونية ومقدمي خدمات استضافة المواقع الإلكترونية، على مَسَار وتخزين والتحكم في كمية كبيرة من البيانات الحاسوبية المتعلقة باتّصالات الإنترنت والمعاملات والمحتوى. ومن ثم يعتبر استخدام سلطات إنفاذ القانون إجراءات قسرية مثل التفتيش والبحث للحصول على هذه البيانات أمرا متعذر التطبيق في أغلب الأحوال، ويرجع ذلك إلى حجم القضايا الفردية الخاضعة للتحقيق وتعطيل الأنشطة التجارية المشروعة. لذلك؛ إصدار الأوامر للأطراف الأخرى للتحقيق في البيانات الحاسوبية يوفر مسارا لإجراءات قانونية كافية للحصول على الأدلة الإلكترونية.

فمن الملاحظ أنه في العديد من الدول، تعتبر هذه الأوامر جائزة في نطاق صلاحيات التحقيق الموجودة، مثل الأوامر العامة بتقديم أي متطلبات يقتضيه مسار التحقيق، أو الأوامر المعنية بالكشف عن إحدى الوثائق. وبالرغم من ذلك؛ يمكن أن تظهر أيضا تحديات إجرائية في هذا الشأن، قد تتمثل في المتطلبات "التقليدية" لتحديد المعلومات بشأن المشتبه بهم قبل إصدار أوامر تتعلق بالأدلة. وفي نطاق التحقيقات في

أمر بشأن بيانات حاسوبية: مثال وطني من دولة في الأمريكتين

في حالة إذا اقتنع القاضي بناء على طلب أحد ضباط الشرطة بأن البيانات الحاسوبية المحددة أو المطبوعة او المعلومات الأخرى تعتبر مطلوبة بشكل مناسب لأغراض أحد التحقيقات الجنائية أو الإجراءات الجنائية، فإنه يجوز للقاضي أن يصدر أمرا لـ:

(أ) أحد الأشخاص في إقليم <الدول> المسيطر على إنتاج أحد الحواسيب من البيانات الحاسوبية المحددة أو المطبوعة أو المخرجات الواضحة الأخرى لتلك البيانات.

(ب) أحد مقدمي خدمة الإنترنت في <دولة> الذي لديه معلومات بشأن الأشخاص المشتركين في الخدمة أو خلافا لذلك.

(ج) أحد الأشخاص في إقليم <الدول> الذي لديه حق الوصول إلى أحد عمليات الحاسوب المحددة وتجميع البيانات الحاسوبية المحددة من الحاسوب وأعطاه إلى شخص محدد.

---

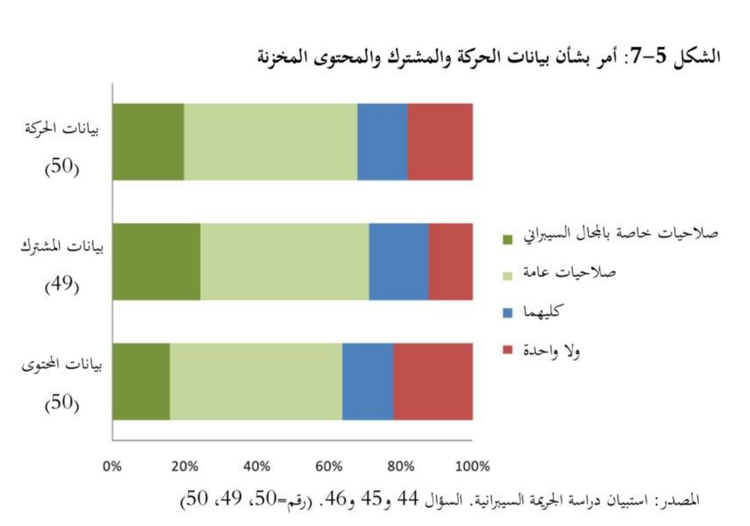
[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 42-51

الجريمة السيبرانية، قد تتمثل المعلومات المعروفة فقط في أحد عناوين برتوكولات الإنترنت أو اتصالات مماثلة قائمة على معلومات، في وقت طلبها من أحد مقدمي خدمة الإنترنت.

ووفقا لذلك؛ تتضمن خمسة صكوك دولية أو إقليمية من الصكوك المعنية بمكافحة الجريمة السيبرانية بأحكام محددة تتعلق بالأوامر الخاصة بالحصول على البيانات المخزنة.[1] وعند القيام بذلك؛ تشير الصكوك بشكل إجمالي إلى التباين – الذي كُشف عنه النقاب سابقا في هذا الفصل – بين "بيانات المشترك"، "بيانات الحركة"، و"بيانات المحتوى". هذا، وعادة ما تتعلق هذه الأحكام بالمعلومات التي تعتبر في حيازة أو تحت سيطرة الشخص أو مقدمي الخدمة. وبالتالي، فإن الأمر يسري فقط على النطاق الذي توجد في البيانات في وقت إصدار الأمر، كما يمكن استرجاعها من قِبَل مُصدر الأمر. ومن الملاحظ أن وجود هذه الصلاحيات التحقيقية مفردة فإنها لا تلزم في حد ذاتها مقدمي الخدمة بجمع المعلومات أو الحفاظ عليها، حيث لن يقوموا خلافا لذلك بمعالجة هذه المعلومات. أما فيما يتعلق "بحركة البيانات"، فإن بعضا من الصكوك[2] متعددة الأطراف تتضمن أيضا آلية للكشف المستعجل جزئيا عن بيانات الحركة بشكل كاف مما يمكن سلطات إنفاذ القانون من تحديد مقدمي الخدمة والمسَار الذي قد أُرسلت من خلاله الرسالة. وقد يعتبر هذا الأمر هاما في حال انخراط عدد مُتَعَدّد من مقدمي الخدمات في معالجة البيانات الحاسوبية أو المراسلات الإلكترونية.

ويظهر الشكل 5–7 أن الصلاحيات العامة، على المستوى الوطني، مرة أخرى معمول بها بين الدول لإجَازَة الأوامر المعنية ببيانات المشترك وحركة البيانات ومحتوى البيانات.[3] وتعتبر نسبة الدول التي توظف أوامر خاصة بالفضاء السيبراني للحصول بيانات المشترك أعلى بقليل من الفئتين الباقيتين من البيانات. إلى جانب ذلك؛ تأثير الصكوك الدولية والإقليمية المعنية بمكافحة الجريمة السيبرانية والذي قد يعكس مطلبا عاما لهذا

الشكل 5–7: أمر بشأن بيانات الحركة والمشترك والمحتوى المخزنة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 44 و45 و46. (رقم=50، 49، 50)

---

[1] مشروع القانون النموذجي للسوق المشتركة لشرق افريقيا والجنوب الأفريقي، المادة (أ) 36؛ القانون النموذجي لدول اتحاد الكومنولث المادة 15، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 18 (1/أ)؛ مشروع النصوص التشريعية للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 22 (هـ)؛ الاتفاقية العربية بشأن مكافحة جرائم المعلومات المادة 25 (1).

[2] مشروع القانون النموذجي للسوق المشتركة لشرق افريقيا والجنوب الأفريقي، المادة (أ/2) 34؛ القانون النموذجي لدول اتحاد الكومنولث المادة 16، اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 17 (1/ب)؛ مشروع النصوص التشريعية للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 24؛ الاتفاقية العربية بشأن مكافحة جرائم المعلومات المادة 24.

[3] الاستبيان الخاص بهذه الدراسة، السؤال رقم 45–47

النمط من البيانات، علاوة على أحد المطالب (المرفوعة نيابة عن مقدمي الخدمة) المتمثلة في وجود صلاحيات وإجراءات قانونية واضحة عند طلب هذه المعلومات.

وهذا ما أيدته تعليقات الدول المجيبة على الاستبيان الخاص بهذه الدراسة. فعلى سبيل المثال؛ ذكرت إحدى دول الأمريكتين أنه بالرغم من أن مقدمي الخدمات غالبا ما يتعاونون مع هيئات إنفاذ القانون طَوْعا، إلا أن تطبيق الأحكام الإجرائية العامة المعمول بها لاستصدار أمر بدعم البيانات اتَّصَفَ بعدم العَمَلِيّة علاوة على التكلفة الباهظة. ولذلك، قد بدأت هذه الدولة بعملية اعتماد حكم خاصّ بالمجال السيبراني للأوامر الخاصة ببيانات المشترك.[1] ومن ناحية أخرى، أفاد عدد قليل من الدول بنجاح استخدام الأحكام العامة. وفي هذا الصدد؛ أوضحت إحدى دول جنوب شرق آسيا، على سبيل المثال، إمكانية تمديد نطاق إحدى الصلاحيات العامة للتحقيق بشأن إصدار أحد الأوامر "لأي وثيقة أو أي شيء أخر". وفي هذا السياق أيضا، أفادت إحدى دول أمريكا الجنوبية أن الصلاحية الممنوحة لأحد القضاة "لفحص المراسلات المخْتُومة" قد تمتد إلى البيانات المخزنة.[2]

أمر بشأن حركة البيانات: مثال وطني من دولة في أوقيانوسيا

الكشف عن حركة البيانات

في حالة ما إذا اقتنع القاضي بناء على طلب أحد ضباط الشرطة بأن البيانات المخزنة المحددة في أحد نظم الحاسوب تعتبر مطلوبة بشكل مناسب لأغراض أحد التحقيقات الجنائية أو الإجراءات الجنائية، يجوز للقاضي أن يستصدر أمرا بأن يكشف الشخص المسيطر على النظام الحاسوبي عن حركة البيانات بشكل كاف والمتعلقة بأحد المراسلات المعَيّنة، وذلك لتحديد:

(أ) مقدمي الخدمة، و

(ب) والمسَار الذي قد أُرسلت من خلاله الرسالة

بصرف النظر عن الشكل القانوني لصلاحيات التحقيق، فإن التفاعل بين هيئات إنفاذ القانون ومقدمي خدمة الإنترنت للحصول على أدلة إلكترونية قد يتسم بالتعقيد البالغ. وتتناول الأقسام اللاحقة من هذا الفصل؛ استخدام الصلاحيات بشكل عملي، فضلا عن التحديات التي جابهتها سلطات إنفاذ القانون في الحصول على البيانات من مقدمي الخدمة، بالإضافة إلى الممارسات الجيدة التي استخدمتها سلطات إنفاذ القانون حيال ذلك.

جمع البيانات في الوقت الحقيقي/آنيا

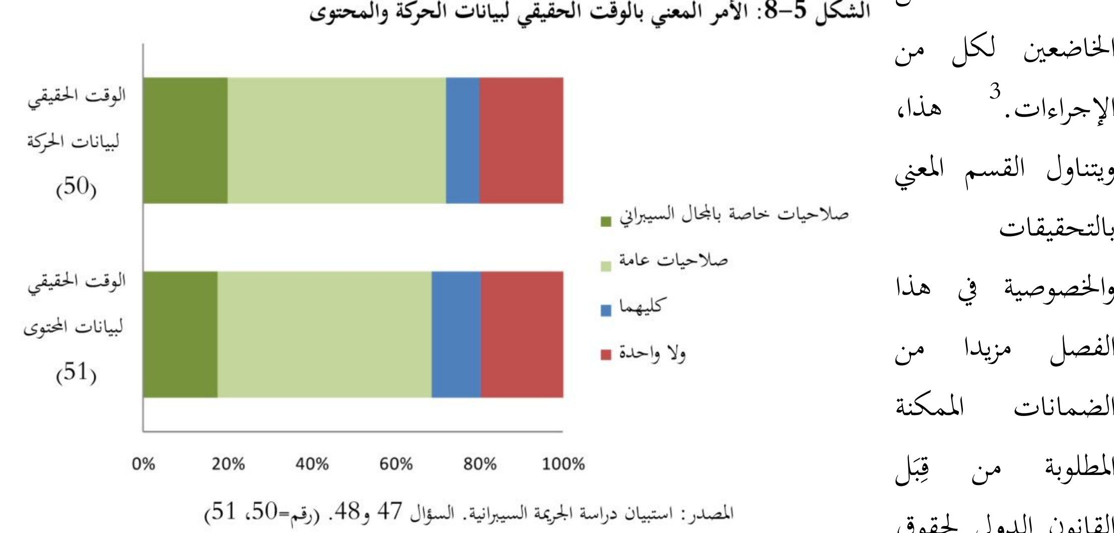
تمثل الأوامر المعنية بالبيانات أحد إجراءات التحقيق للحصول على البيانات الحاسوبية المخزنة. ومع ذلك، لَن تخزن أيضا الأدلة الإلكترونية الأسَاسِيّة على الإطلاق (الموجودة فقط في نطاق المراسلات العابرة)، أو تتطلب الوقت الفعلي لجمع البيانات، ويرجع ذلك إلى الحاجة الملِحَّة لإحدى التحقيقات التي تضطلع بإجرائها إحدى هيئات إنفاذ القانون، أو دقتها أو صعوبتها.

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 42-51.

[2] الاستبيان الخاص بهذه الدراسة، السؤال رقم 42-51.

ووفقا لذلك؛ تتضمن ستة من الصكوك الدولية أو الإقليمية أحكاما بشأن الوقت الحقيقي لجمع البيانات الحاسوبية. ونحو ذلك؛ فإن الصكوك بشكل إجمالي تُميز بين الوقت الحقيقي لبيانات الحركة[1] والوقت الحقيقي لبيانات المحتوى.[2] ويتعلق هذا التمييز، ليس على الأقل، باختلافات على مستوى التَدَخّل في الحياة الخاصة للأشخاص الخاضعين لكل من الإجراءات.[3] هذا، ويتناول القسم المعني بالتحقيقات والخصوصية في هذا الفصل مزيدا من الضمانات الممكنة المطلوبة من قِبَل القانون الدولي لحقوق الإنسان. وفي هذا الصدد؛ يشير أحد الصكوك الدولية (اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية) صراحة إلى اعتراض محتوى البيانات المتعلقة "بمجموعة من الجرائم الجسيمة التي يحددها القانون المحلي".[4] ومن منظور عملي؛ غالبا ما تصوّر الصكوك متعددة الأطراف أن الوقت الحقيقي لجمع البيانات يمكن تنفيذه إما بشكل مباشر من قبل سلطات إنفاذ القانون من خلال تطبيق وسائلها التقنية الخاصة بها، أو عن طريق إرغام أحد مقدمي الخدمات ضمن قدراتهم التقنية الموجودة لجمع البيانات الحاسوبية أو تسجيلها، أو للتعاون ومساعدة السلطات في أداء ذلك.

الشكل 5-8: الأمر المعني بالوقت الحقيقي لبيانات الحركة والمحتوى



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 47 و48. (رقم=50، 51)

---

[1] مشروع القانون النموذجي للسوق المشتركة لشرق افريقيا والجنوب الأفريقي، المادة 38؛ القانون النموذجي لدول اتحاد الكومنولث المادة 19؛ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 20؛ مشروع النصوص التشريعية للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 25؛ الاتفاقية العربية بشأن مكافحة جرائم المعلومات، المادة 28.

[2] مشروع اتفاقية الاتحاد الأفريقي، المواد 3-53؛ مشروع القانون النموذجي للسوق المشتركة لشرق افريقيا والجنوب الأفريقي، المادة 39؛ القانون النموذجي لدول اتحاد الكومنولث المادة 18؛ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 21؛ مشروع النصوص التشريعية للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 26؛ الاتفاقية العربية بشأن مكافحة جرائم المعلومات، المادة 29.

[3] See Walden, I. *Addressing* the Data Problem: The Legal Framework Governing Forensics in an Online Environment. *Second International Conference iTrust 2004*, Proceedings. Oxford, 29 March-1 April 2004.

[4] اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 20

على المستوى الوطني، أفاد ما يقرب من نسبة 40 في المائة من الدول المجيبة على الاستبيان الخاص بهذه الدراسة بأنه قد تم استخدام إحدى الصلاحيات العامة للتحقيق للتصَرّيح بماهية الوقت الحقيقي لاعتراض حركة البيانات ومحتوي البيانات. هذا، وقد أشار عدد من الدول، على سبيل المثال، إلى تمديد نطاق "اعتراض أعمال الاتصالات السلكية واللاسلكية" العامة، أو "قوانين التَنَصّت" للوقت الحقيقي لجمع البيانات الحاسوبية.[1] وبشكل إجمالي؛ أفادت أكثر من نسبة 60 في المائة من الدول المجيبة بوجود صلاحية قانونية للوقت الحقيقي لجمع البيانات، إما من خلال صلاحية عامة أو صلاحية خاصة بالمجال السيبراني. ومن ناحية أخرى؛ أبرزت بعض الدول تطبيق ضمانات على هذه الصلاحيات، بما فيها تحديد الوقت الحقيقي لجمع محتوى البيانات للجرائم الجسيمة فقط.[2]

جمع البيانات في الوقت الحقيقي: مثال وطني من دولة في غرب آسيا

الوقت الحقيقي لجمع بيانات الحركة

1. يُفَوّض أحد وكلاء النائب العام في تقديم طلب إلى إحدى المحاكم صاحبة الاختصاص المكاني بالتحقيق لاستصدار أمر لجمع بيانات الحرمة آنيا، وبناء على ذلك يلتزم مقدم الخدمة بالتعاون مع هيئة التحقيق مع تقديم المساعدة لها في تحديد الوقت الحقيقي لجمع حركة البيانات أو تسجيلها والمترابطة بمراسلات محددة تم إعدادها ونقلها عبر أحد أنظمة الحاسوب داخل الإقليم، متى كان هناك سبب محتمل بأن أحد الأشخاص يستعمل نظام حاسوبي لارتكاب جريمة...
2. تعتبر المقترحات المنصوص عليها في الفقرة 1 في المادة الحالية بمثابة قدرة تقنية لمقدم الخدمة لتحديد الوقت الحقيقي لجمع حركة البيانات أو تسجيلها. لا يجوز أن تتجاوز مُدّة "الوقت الحقيقي لجمع حركة البيانات أو تسجيلها" المدّة الضرورية لجمع الأدلة في القضية الجنائية.
3. تنظر المحكمة في المقترحات المنصوص عليها في الفقرة 1 و2 من هذه المادة طبقا للإجراء الوارد في المادة <...> من هذا القانون.

وفيما يتعلق بالتطبيقات العملية لاعتراض البيانات، فإنه في أغلب الأحيان يتم التمييز بين مقدمي الخدمة العام ومقدمي الخدمة الخاص. فعلى سبيل المثال؛ تنص إحدى التشريعات الوطنية لدولة من دول غرب أوروبا على أن اعتراض البيانات الحاسوبية من قِبَل المقدمين العموميين يعتبر اعتراضا بالتعاون مع مقدمي الخدمة، ما لم يكن هذا التعاون غير ممكن أو يعتبر مخالفا لمصالح التحقيق. أما فيما يتعلق بمقدمي الخدمة غير العامة، فتنص التشريعات الوطنية على "منح" مقدم الخدمة الفرصة للتعاون في الاعتراض، ما لم يكن هذا مستحيلا أو غير مرغوب فيه.[3]

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 47 و48.

[2] المرجع السابق.

[3] Koops, B-J. 2010. Cybercrime legislation. *Electronic Journal of Comparative Law*, 14(3).

استخدام أدوات التحاليل الجنائية الحاسوبية عن بُعد

توفر مجموعة الأدوات التكنولوجية لهيئات إنفاذ القانون إمكانيات لكل من جمع الأدلة بشكل مباشر من نظم الحاسوب عن بُعد، وجمع معلومات استخباراتية أو معلومات تتعلق بالتحقيق بشكل عام. فهذه الأدوات مثل برامج رصد لوحة المفاتيح وإدارة البرامج عن بُعد، وعندما توضع مثل هذه الأدوات في جهاز أحد المشتبه بهم فإن بإمكانها نقل معلومات عن بُعد بشأن نشاط لوحة المفاتيح والبيانات الحاسوبية المخزنة –أو البيانات المرسلة أو البيانات المستقبلة– بواسطة الجهاز.[1] نظرا إلى مجموعة المعلومات الشخصية المخزنة على أجهزة الحاسوب، فإن استعمال هذه الأدوات تمثل انْتِهاكا جَسِيما للحياة الخاصة للأشخاص الفاعلين محل التحقيق. ومن وجهة نظر الإثبات؛ فالحصول على الأدلة عبر استخدام أدوات عن بُعد بشأن "حياة" نظم الحاسوب قد تفتح أيضا أبواب التحدي. وفي هذا الصدد على سبيل المثال؛ يجب توضيح أن العمليات التي يضطلع بها المحَقّق لا تغير بحد ذاتها من حالة النظام الحاسوبي قيد التحقيق.[2]

برمجيات التحاليل الجنائية عن بُعد: مثال وطني من دولة في أوقيانوسيا

يخوّل تفتيش الشيء عن بعد بأمر تفتيش

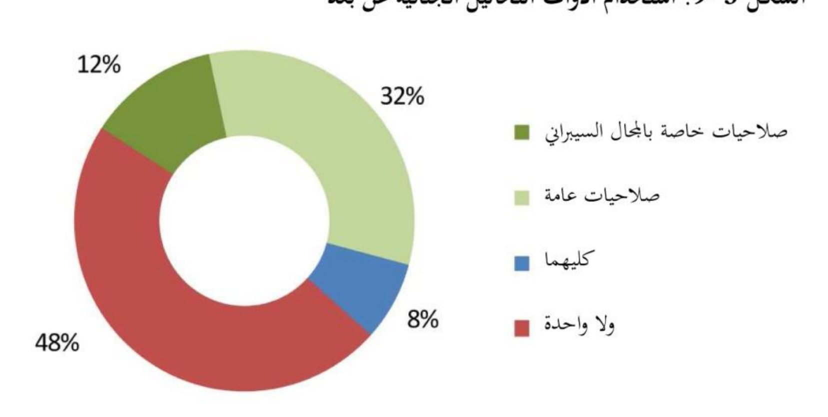
يجوز لأي شخص ينفذ أمرا بالتفتيش؛ يُخَوّل البحث المتاح عن بُعد، أن

(أ) يستعمل تدابير مناسبة للوصول إلى الشيء موضوع التفتيش؛ و

(ب) في حالة خضوع أي من المواد غير المادية في الشيء للبحث، أو للمصادرة خلافا لذلك، تنسخ هذه المادة (وذلك عن طريق المعاينة، الاستنساخ أو أساليب التحليل الجنائي الأخرى).

يشير أحد الصكوك الدولية أو الإقليمية (غير الملزمة) إلى استخدام أدوات التحاليل الجنائي عند بُعد، كأحد إجراءات التحقيق. وفي هذا الصدد تنص المادة (27) من مشروع النصوص التشريعية للاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات على أنه يجوز للقاضي تفويض أحد ضباط الشرطة في اسْتَخْدَام "*برنامج تحليل جنائي عن بُعد*" لإحدى المهام المحددة المطلوبة لأغراض التحقيق. وبشكل عام؛ أيضا تشير اتفاقية مجلس

الشكل 5–9: استخدام أدوات التحاليل الجنائية عن بعد



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 50. (رقم=40)

[1] See, for example, Gartner. 2012. *Remote Forensics Report 2012*.

[2] Hay, B., Nance, K., Bishop, M. 2009. Live Analysis: Progress and Challenges. *IEEE Security and Privacy*, 7(2):32

أوروبا لحماية الطفل (المادة 30 (5)) إلى الالتزام باتخاذ التدابير التشريعية الضرورية والتدابير الأخرى التي تجيز إمكانية القيام" *بعمليات سرية*".

أكثر من ثلث الدول المجيبة على الاستبيان الخاص بهذه الدراسة لم يقدموا إجابة بشأن وجود تشريع يجيز استعمال أدوات التحاليل الجنائية الحاسوبية عن بُعد في التحقيقيات التي تضطلع بإجرائها سلطات إنفاذ القانون. وفي حين أفادت إحدى هذه الدول بأنها فعلت ذلك، إلا أن نصف الدول تقريبا أفاد بعدم وجود هذه الصلاحية. أما فيما يتعلق بالنصف الآخر من الدول المجيبة، فقد أشار إلى أن هذه الصلاحيات تم إدراجها في التشريع، حيث أشارت الأغلبية منها إلى الصلاحيات العامة، بدلا من الصلاحيات الخاصة بالمجال السيبراني. بيد أن التعليقات التي أبدتها الدول قد تراوحت" *ما بين التصريح صراحة بعدم وجود أحكام تشريعية تعنى باستخدام أدوات التحاليل الجنائية الحاسوبية عن بُعد، إلى التأكيد على أن القانون الوطني يجيز تركيب جهاز مراقبة للبيانات*". [1] وأخيرا؛ علقت الدول الأخرى، بشكل عام، بأن الأطر الإجرائية في ظروف مُعَيّنة تنص على استعمال "الخبرة التقنية أو العلمية"، بغية الحصول على المعلومات المطلوبة أثناء التحقيق. [2]

وصول هيئات إنفاذ القانون المباشر إلى البيانات الموجودة خارج نطاق إقليمها

تعني الموصولية العالمية أن البيانات الحاسوبية ذات الصلة بالتحقيقات التي تجريها سلطات إنفاذ القانون تعتبر متواجدة بشكل متزايد خارج الحدود الإقليمية للولاية القضائية القائمة بالتحرّيات، سواء كانت جريمة عامة أو جريمة سيبرانية. وعلى النحو الذي تمت مناقشته في الفصل السابع (التعاون الدولي)، فإن الوسائل التقليدية الرسمية للتعاون الدولي لم تعد كافية في وقته لضمان الوصول إلى بيانات عابِرة تجاوزت الحدود الإقليمية. واعترافا بهذا التحدي؛ تتضمن ثلاثة من الصكوك الدولية أو الإقليمية أحكاما بشأن الوصول إلى البيانات الحاسوبية عبر الحدود3. وتصور هذه الأحكام بشكل نموذجي أن سلطات إنفاذ القانون يجوز لها الوصول أو تلقي–من خلال أحد النظم الحاسوبية الموجودة في الإقليم الوطني– بيانات حاسوبية مخزنة موجودة في دولة أخرى بموجب موافقة قانونية أو موافقة إرادية من أحد الأشخاص الذين لديهم السلطة القانونية للكشف عن البيانات. [4]

---

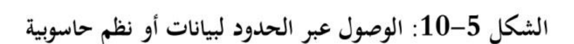
[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 42-51

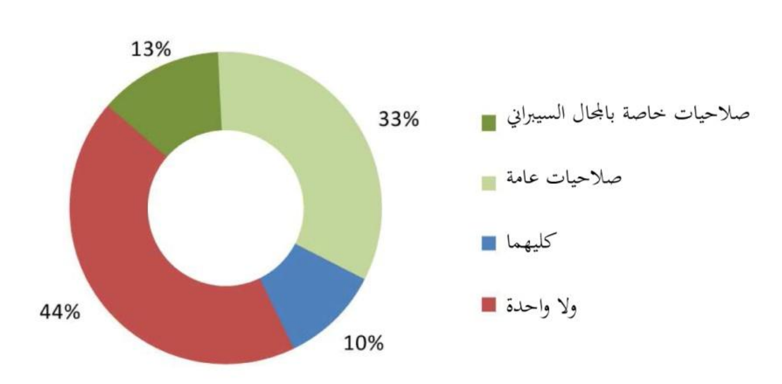
[2] المرجع السابق

3 أنظر مشروع القانون النموذجي للسوق المشتركة لشرق إفريقيا والجنوب الأفريقي، المادة 49/ب؛ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 32/ب؛ الاتفاقية العربية بشأن مكافحة جرائم المعلومات، المادة 40/ب

[4] عادة ما تميز الأحكام بشأن الوصول إلى البيانات الحاسوبية عبر الحدود بين الوصول إلى المواد المتاحة للجمهور (مفتوحة المصدر) والمواد الأخرى، حيث أصبح الوصول إلى مواد المصادر المفتوحة لأغراض العدالة الجنائية من قبيل الممارسات المقبولة بشكل عام. (انظر مجلس أوروبا 2012، الولاية القضائية والوصول عبر الحدود الإقليمية: ماهية الخيارات؟ تقرير الفريق العامل عبر الحدود–الذي اعتمده *T-CY* في 6 كانون الأول/ديسمبر2012. استعمال مصطلح الوصول "عبر الحدود" في هذه الدراسة يعني لذلك الوصول إلى مواد المصادر المغلقة.

كما هو الحال مع استخدام أدوات التحليل الجنائي عن بُعد؛ لم يجب أكثر من الدول المجيبة على الاستبيان الخاص بهذه الدارسة على السؤال المتعلق بوجود صلاحيات للوصول "عبر الحدود". بيد أن إحدى هذه الدول قامت بذلك، حيث أشار أكثر من نصف الدول إلى وجود مثل هذه الصلاحية. ومع ذلك، فمن الملاحظ أن الدول قد فسرت المصطلح على نطاق واسع ليستوعب أيضا الموقف حيث يتم الحصول على الموافقة بشأن الإجراء من سلطات الدولة التي قد نفذت الإجراء. فعلى سبيل المثال؛ يجيز تشريع إحدى الدول إصدار أمر قضائي يسمح بتركيب أجهزة مراقبة في "الأماكن/الأشياء الخارجية". ومع ذلك؛ قد يمكن فعل ذلك فقط إذا "اقتنع القاضي مصدر الأمر بأنه تمت الموافقة على المراقبة من قِبَل أحد المسؤولين في الدولة الأجنبية والذي أيد ذلك بشكل كاف"[1]. وأخيرا، فقد ذكرت بعض الدول إلى أن صلاحيات الوصول "عبر الحدود" في القانون الوطني، مشار إليه في تعليقات مكتوبة لاستعمال الصكوك المعنية بالمساعدة القانونية المتبادلة. وبالتالي؛ فإن النسبة الإجمالية للدول التي أفادت بوجود سلطة تشريعية للوصول "عبر الحدود" خلال الاستبيان المرافق لهذه الدراسة، قد تعتبر أكبر من مجموعة الدول التي لديها صلاحية للسماح بالوصول "عبر الحدود" بشكل أكثر صرامة (أي دون ترخيص من السلطات الوطنية) على النحو المتوخى من بعض الصكوك الدولية والإقليمية.


الشكل 5-10: الوصول عبر الحدود لبيانات أو نظم حاسوبية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 51. (رقم=39)

هذا ويتناول الفصل السابع (التعاون الدولي) المسائل المتعلقة بوصول سلطات إنفاذ القانون المباشر إلى البيانات خارج الحدود الإقليمية بمزيد من التعمق، بما في ذلك الاستخدام العملي لهذه الإجراءات من قِبَل الشرطة.

استعراض

يكشف استعراض الأساس القانوني لصلاحيات التحقيق المستخدمة في الجريمة السيبرانية (وفي الواقع، لأي جريمة تنطوي على أدلة إلكترونية) تعددا كبيرا في النهج المستخدم على المستوى الوطني. وهذا يشتمل على ما يتعلق بالنطاق الذي يمكن معه تفسير الصلاحيات "التقليدية" لتطبيقها على البيانات غير المادية، فضلا عن وجود نطاق للسلطة القانونية للإجراءات التدخلية بشكل خاص، مثل استخدام التحاليل الجنائية عن بُعد في التحقيقات. وتظهر النُهُج الوطنية، بشكل إجمالي، لصلاحيات التحقيق في الجريمة السيبرانية قواسم مشتركة بشكل

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 42-51.

أقل من تجريم العديد من أفعال الجريمة السيبرانية. بالرغم من ذلك، وبينما تتسم الصلاحيات القانونية بالتنوع، إلا أن ذلك يُظهر درجة جيدة من التوافق بشأن وجود أنواع من إجراءات التحقيق والتي يجب أن تكون متاحة. ومن الملاحظ أن هناك توافقا وتماثلا لتلك الصلاحيات الواردة في العديد من الصكوك متعددة الأفراد؛ ومنها: (1) الصلاحيات المعنية بالتفتيش والمصادرة، (2) الصلاحيات المعنية بالحصول على البيانات الحاسوبية المخزنة، (3) الصلاحيات المعنية بالوقت الحقيقي لجمع البيانات، و(4) صلاحيات تكفل التحفظ المعجل على البيانات.

بالإضافة إلى الأساس القانوني لهذه الصلاحيات، يجب النظر في مسألتين: (أ) ماهية الحدود والضمانات التي يجب تطبيقها على هذه الصلاحيات، و(ب) استعمال صلاحيات التحقيق بشكل عملي. هذا، ويتناول القسم التالي من هذا الفصل ماهية الحدود والضمانات التي ارتأتها معايير حقوق الإنسان الدولية بشأن الخصوصية، في حين يتناول القسم اللاحق استعمال إجراءات التحقيق بشكل عملي.

3-5 الخصوصية وإجراءات التحقيق

الاستنتاجات الرئيسية:

- تفيد تقريبا جميع الدول المجيبة على الاستبيان الخاص بهذه الدراسة بأن الخصوصية القائمة على الحمايات تعتبر سارية في سياق البيانات الحاسوبية والمراسلات الإلكترونية
- تفيد الدول بوجود مجموعة كبيرة من الضمانات لحماية الخصوصية أثناء تحقيقات هيئات إنفاذ القانون، تشتمل على القيود بشأن البيانات التي يمكن الوصول إليها، الحدود الزمنية، متطلبات "السبب المحتمل"، وإشْراف القضاء والنيابة العامة
- يحدد القانون الدولي لحقوق الإنسان بشكل واضح مجموعة من الحمايات لخصوصيات الأشخاص الذين يخضعون لتحقيقات هيئات إنفاذ القانون. وتتضمن المبادئ الأساسية وجوب أن تعطي صلاحيات التحقيق مؤشرا واضحا للأوضاع والظروف التي قد تُستعمل بموجب هذه الإجراءات، وذلك جنبا إلى جنب مع ضمانات فعالة ضد إساءة استعمال مثل هذه الصلاحيات
- تطوير الحوسبة السحابية يطرح درجة عالية من الغُمُوض للمستخدمين فيما يتعلق بنظام الخصوصية الذي سيطبق على بياناتهم، بالإضافة إلى الظروف التي تجعل التدخل في الخصوصية أمرا مشروعا لأغراض التحقيقات التي تجريها هيئات إنقاذ القانون أو بهدف المراقبة الأمنية

حقوق الإنسان وتحقيقات سلطات إنفاذ القانون

تتمثل إحدى شواغل القانون الدولي لحقوق الإنسان في الطرائق التي تنتهجها الدول في مكافحة الجريمة وتحقيق أهداف العدالة الجنائية.[1] ومن المستقر؛ أن هناك إمْكانيّة لارتباط معايير حقوق الإنسان بكل جوانب التحقيق والملاحقة القضائية للجريمة وقانون الإجراءات الجنائية، والممارسة، ومن ثم يَتَبّع القانون الدولي لحقوق الإنسان بشكل خاص كل هذه المعايير.[2]

فهناك مجموعة من الحقوق ربما تُطبق على التحقيقات التي تضطلع بإجرائها سلطات إنفاذ القانون، ومنها حق الشخص في الحرية والأمان، والحقوق المتعلقة بالمحاكمة العادلة.[3] ومع ذلك؛ تظهر غالبا تحديات في هذا المجال، تتعلق بالخصوصية القائمة على الحمايات في إطار القانون الدولي والقانون الوطني.

وتتضمن كل الصكوك الدولية كالعهد الدولي الخاص بالحقوق المدنية والسياسية، والاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية، والاتفاقية الأمريكية لحقوق الإنسان، محظورات بشأن التدخل التعسفي في الخصوصية والأسرة والمنزل والمراسلات.[4] ويتمتع نطاق "الخصوصية" بمفهوم واسع[5] وفقا للقانون الدولي والسوابق القضائية، ومن الواضح أن الطبيعة التدخلية للتحقيقات الجنائية سترتبط بخصوصية قائمة على حقوق[6] تندرج حيث لا يدرك المشتبه به أن المعلومات يتم جمعها،[7] وبشكل مُتَجَانِس؛ إذا كان التشريع القائم الذي يمنح صلاحيات للتحقيق مُجَرّد تهديد.[8]

فعلى النحو المعمول به في الحقوق الأخرى؛ فإن حقوق الخصوصية في القانون الدولي ليست حقوقا مطلقة بيد أنها تخضع لقيود، بما في ذلك القيود الواردة في الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية، ولاسيما القيد المعنى بـ "حفظ النظام ومنع الجريمة".[9] وفي هذا الصدد؛ تعتبر الضمانات الواردة في قانون الإجراءات الجنائية مثل: تحديد الأوضاع والحالات التي يمكن معها استعمال صلاحيات الحقيق، تحديد المسؤولين المفوضين،

---

[1] لجنة الأمم المتحدة المعنية بالمخدرات ولجنة الأمم المتحدة لمكافحة الجريمة والعدالة الجنائية 2010. مراقبة المخدرات ومنع الجريمة والعدالة الجنائية من منظور حقوق الإنسان. مذكرة من المدير التنفيذي E/CN.7/2010/CRP.6 – E/CN.15/2010/CRP.1 3 آذار/مارس 2010

[2] Colvin, M., and Cooper, J. (eds.) 2009. *Human Rights in the Investigation and Prosecution of Crime.* Oxford: Oxford University Press.

[3] المادتان 9 و14 من العهد الدولي الخاص بالحقوق المدنية والسياسية

[4] المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، والمادة 8 من الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية، والمادة 11 من الاتفاقية الأمريكية لحقوق الإنسان.

[5] أُنظر على سبيل المثال؛ لجنة الأمم المتحدة لحقوق الإنسان 1988، التعليق العام رقم 16: الحق في احترام الخصوصية والعائلة والمنزل والمراسلات، وحماية الشرف والسمعة، 8نيسان/أبريل 1998.

[6] See for example, United Nations Human Rights Committee. *Communication CCPR/C/82/D/903/1999*; IACtHR *Tristán Donoso*. Judgement of 27 January 2009; and ECtHR Application No's 35394/97 and 13710/88.

[7] أُنظر المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 79/8691

[8] أُنظر المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 00/54934

[9] أُنظر الفقرة (2) من المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية، والتي تنص على أن "لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقا للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحرياتهم"

الطريقة التي يصدر بها التصريح، ومِقْدار المدة الزمنية التي يمكن تطبيقها على إجراءات التحقيق، أمرا حيويا لتقييم حقوق الإنسان عما إذا كانت التحقيقات الجنائية التي تنتهك الخصوصية تعتبر مقبولة في نطاق الضرورة المشروعة.[1]

ومتى تعلق الأمر بالتحقيق في الجريمة السيبرانية، فإنه يجب تقييم كل إجراء من إجراءات التحقيق في سياقه القانوني والعملي، وذلك لتحديد ما إذا كان للمتدخل في الخصوصية أو العائلة أو المنزل أو المراسلات له ما يبرره للتدخل. وفي هذا الإطار؛ غالبا ما تثير طبيعة المراقبة السرية و/أو الإلكترونية كأحد أساليب التحري في الجريمة السيبرانية تحديات مُعَيّنة للخصوصية،[2] إلا أنه من الهام التذكر بأن متطلبات التَوَافُق لحقوق الخصوصية تسري بشكل متساو على إجراءات التفتيش والمصادرة "الاعتيادية".[3] وبالتالي، يجب أن تعكس الحدود والضمانات الواردة في القانون الإجرائي التدخل التبايني لإجراءات التحقيق، مع ضمان أن كل إجراء يتم استخدامه فقط في متى اقتضى الأمر ذلك في أحد المجتمعات الديمقراطية.

وجود حماية خصوصية وضمانات إجرائية

خلال جمع المعلومات الخاصة بهذه الدراسة، أجابت الدول على الأسئلة المعنية بالحماية القانونية للخصوصية في سياق البيانات الحاسوبية أو المراسلات الإلكترونية، وكيف توظف حقوق الخصوصية كضمانات أثناء تحقيقات سلطات إنفاذ القانون. كما سُئلت الدول أيضا عن ماهية الظروف التي يمكن فيها تقييد حقوق الخصوصية لأغراض الكشف والتحقيق في الجريمة السيبرانية، إلى جانب ماهية العناصر ذات الصلة بحقوق الخصوصية خارج نطاق الولاية القضائية والتعاون الدولي.

أشارت تقريبا كافة الدول المجيبة على الاستبيان إلى أن حماية الخصوصية تعتبر معمولا بها في سياق البيانات الحاسوبية والمراسلات الإلكترونية. ومع ذلك، فإن طريقة الحماية التي يتناولها القانون قد أظهرت اختلافات كثيرة. كما أشار العديد من الدول إلى حقوق الخصوصية الدستورية الشامِلة التي طبقت أيضا على البيانات الحاسوبية، كما أن عددا قليلا من الدول سلط الضوء على نهج "محايد من الناحية التكنولوجية" للحق في الخصوصية في تشريعاتهم الوطنية. في حين ذكرت الدول الأخرى تشريعات محددة تتضمن أعمال "الخصوصية"؛

[1] يتمثل النهج العام الذي اعتمدته لجنة الأمم المتحدة لحقوق الإنسان في التساؤل ما إذا كان التدخل في الخصوصية يعتبر منصوص عليه قانونا، ويتفق مع الأحكام والأهداف والغايات الواردة في العهد الدولي الخاص بالحقوق المدنية والسياسية، كما يعتبر من المناسب في الظروف الخاصة للحالة (انظر لجنة الأمم المتحدة لحقوق الإنسان، البلاغ رقم *CCPR/C/82/D/903/1999* ولجنة الأمم المتحدة لحقوق الإنسان، التعليق رقم 16). أما نهج المحكمة الأوروبية لحقوق الإنسان في القضايا التي يضطلع بالتحقيق فيها هيئات إنفاذ القانون يتمثل في توجيه سؤال يتعلق بـ (1) ما إذا كان هناك تدخل في حقوق الخصوصية المحمية بموجب المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية؛ (2) ما إذا كان هذا التدخل كان وفقا للقانون، ويشتمل ذلك ليس فقط على الأسس في القانون المحلي، بل أيضا "نوعية" القانون من حيث إمكانية الوصول إليه، وتبصره بعواقب الأمور قبل وقوعها، وتوافقه مع مبدأ سيادة القانون، و(3). ما إذا كان التدخل ضروريا في مجتمع ديمقراطي (انظر المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 00/62540).

[2] انظر على سبيل المثال، مكتب الأمم المتحدة المعني بالمخدرات والجريمة 2009. الممارسات الحالية في المراقبة الالكترونية في التحقيق في الجرائم الخطيرة والمنظمة.

[3] انظر على سبيل المثال؛ المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 88/13710.

قوانين "حماية الخصوصية"؛ أعمال "تنظيم الاتصالات (السلكية واللاسلكية)"؛ أعمال "حماية الخصوصية في المراسلات الإلكترونية"؛ جرائم انتهاك الخصوصية في "القانون الجنائي"؛ قوانين سرية المراسلات"؛ و"الأعمال المتعلقة بمحتوى أسْرَار المراسلات".[1] ومن الملاحظ أن بعض الدول اتخذت الصكوك الدولية – كالاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية – كأحد مصادر الحماية الوطنية. بيد أن عددا قليلا من الدول ذكر صراحة بأن ليس لديها قانونا "عاما" يتعلق بالخصوصية، وبالرغم من ذلك، فإن هذه الدول استفادت من حماية البيانات الحاسوبية والمراسلات الإلكترونية في هذه الدول، مثل قوانين السرية والامتيازات المهنية القانونية.[2]

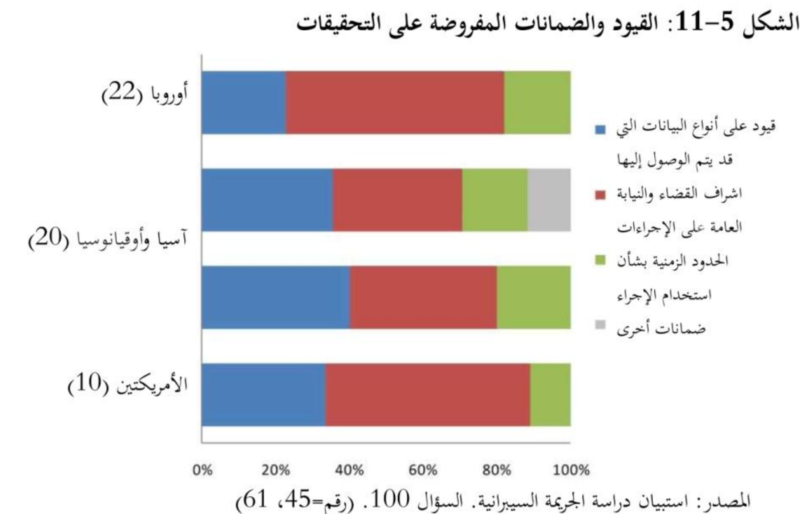
وفي هذا السياق أيضا؛ أكد عدد من الدول أن حماية الخصوصية معمول بها في سياق التحقيقات التي يضطلع بإجرائها سلطات إنفاذ القانون، بيد أنها أبرزت أن الخصوصية يجب أن تكون متوازنة نظير الحاجة إلى منع الجريمة والتحقيق فيها. وبينما وصفت بعض من الدول كيفية تحقيق هذا التوازن، إلا أن غالبية الدول أشارت فقط إلى ماهية متطلبات إصدار الأوامر، أو متطلبات كل من السلطة القضائية أو النيابة العامة، للتفتيش الاقتحامي أو الرَقَابَة. وجدير بالذكر؛ أن إحدى الدول سلطت الضوء على أن القانون الوطني حدد أنه *"يتعين إيلاء العناية الواجبة [أثناء عمليات البحث والمصادرة] بغية منع الكشف عن المراسلات الخاصة التي لا ترتبط بالإجراءات الجنائية المتخذة".*[3] إلى جانب ذلك، فإن إحدى الدول الأخرى ذكرت أيضا أنه يجب استخدام التنصت على الاتصالات فقط كوسيلة "تكميلية" لتيسير أعمال التحقيق الجنائي. هذا، وأوضحت بعض الدول بشكل خاص أن قوانين حماية البيانات (التي يعتبر أداؤها أمرا هاما لحماية الخصوصية في سياق البيانات الشخصية المراقبة والمعالجة من الأطراف الأخرى) متضمنة استثناءات تسمح، على سبيل المثال، للأطراف الثلاثة بالكشف عن المعلومات إلى إحدى هيئات إنفاذ القانون في حالة وجود "ضرورة مناسبة" لتنفيذ القانون الجنائي.[4]

وقد توجه الاستبيان الخاص بهذه الدراسة بطلب إلى الموظفين المكلفين بإنفاذ القانون لتقديم مزيد من التفاصيل بشأن طبيعة الضمانات الإجرائية التي تساعد في تأمين حقوق الإنسان واحترام الخصوصية أثناء عمليات التحقيق. وفي الرد على هذا السؤال؛ قد أفادت أَكْثَرِيّة الدول (85 في المائة) بوجود حدود وضمانات وطنية لإجراءات التحقيق التي تضطلع بها سلطات إنفاذ القانون بشأن الجريمة السيبرانية.[5] وبناء على ذلك، فإن ما يدعو للاستغراب أن عددا قليلا من الدول ذكرت عدم وجود ضمانات، مما يعتبر ذلك حالة قد تؤدي إلى عدم التوافق مع القانون الدولي لحقوق الإنسان.

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 21.
[2] المرجع السابق.
[3] المرجع السابق.
[4] المرجع السابق.
[5] الاستبيان الخاص بهذه الدراسة، السؤال رقم 100

وقد تجسدت الضمانات التي ذكرتها الدول في شكل قيود على أنواع البيانات الحاسوبية التي قد يتم الوصول إليها من قِبَل سلطات إنفاذ القانون، فضلا عن إشراف المحكمة أو النيابة العامة على إجراءات التحقيق. وأشارت أيضا بعض الدول إلى الحدود الزمنية المفروضة على استخدام إجراءات التحقيق.[1] وفي هذا الصدد أيضا، استشهدت الدول الأخرى بأنظمة للحماية تتضمن قيودا على الوصول إلى البيانات الحاسوبية بمجرد حصول سلطات إنفاذ القانون عليها، قيود على استخدامها، المتطلبات المتعقلة بعدم إتْلافها، إلى جانب آليات مستقلة للرقابة الداخلية.[2] وأفادت إحدى الدول أن *"الحدود والضمانات التعددية الواسعة، مع القيود المختلفة والأنظمة الوقائية مُطَبّقة على كل صلاحية من صلاحيات الوصول إلى (بيانات الاتصالات السلكية واللاسلكية، المحتوى المخزن، والمحتوى المباشر). هذا، وتتضمن هذه الأنظمة الوقائية: متطلبات يجب تحقيقها قبل منح الوصول، وقيود على الوصول مجرد منحه، وقيود على استعمال المواد بمجرد الوصول، ومتطلبات عدم التعرض، وأنظمة مستقلة للرقابة الداخلية، ومتطلبات إبلا غ العامة."*[3]

الشكل 5–11: القيود والضمانات المفروضة على التحقيقات



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 100. (رقم=45، 61)

وصرحت غالبية الدول (ما يزيد عن نسبة 75 في المائة) أن الضمانات قد وردت في التشريع الأساسي، بينما أفادت باقي الدول بأن الضمانات مشتقة من تشريعات فرعية مثل مرسوم حكومي، وقرارات المحاكم أو سياسيات الملاحقات القضائية التي تضطلع بها هيئات إنفاذ القانون.[4] وبينما تستمد الضمانات شرعيتها من مصادر غير التشريعات الرئيسية، إلا أنها يجب أن تظل – كما هو مبين أدناه – مكرسة في "القانون" الذي ينص على ضمانات كافية وفعالة لمكافحة إساءة استعمال إجراء التحقيق بحد ذاته.

---

[1] المرجع السابق.

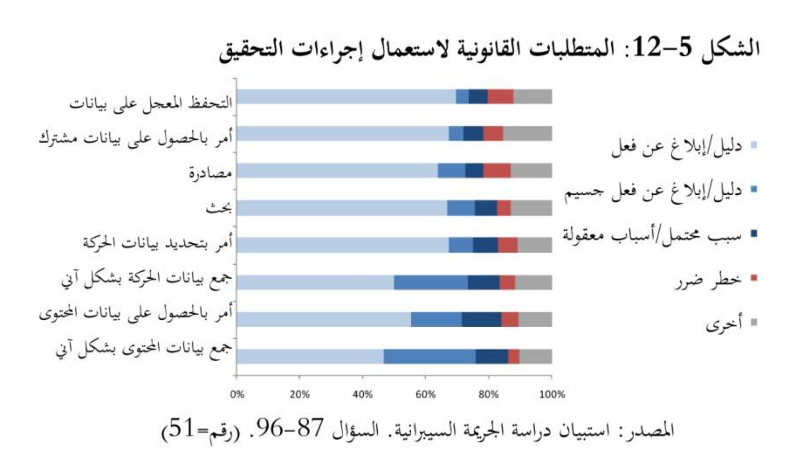
[2] المرجع السابق. بالإضافة إلى ذلك، يجب ملاحظة أن دول الاتحاد الأوروبي تعتبر خاضعة إلى القرار الإطاري للمجلس الأوروبي 2008/977/JHA، الصادر في 27 تشرين الثاني/نوفمبر 2008 بشأن حماية البيانات الشخصية المعالجة في إطار تعاون الشرطة والقضاء في المسائل الجنائية، والتي تنظم عملية معالجة البيانات الشخصية من قبل هذه السلطات.

[3] الاستبيان الخاص بهذه الدراسة، السؤال رقم 100

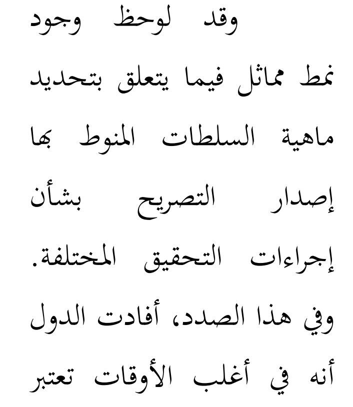
[4] المرجع السابق.

وقد طُلب من الدول أيضا أن تقدم مزيدا من التفصيل بشأن ماهية الضمانات الإجرائية المحَدّدة، وكذلك الطبيعة القانونية للمتطلبات التي يتعين استيفاؤها قبل استخدام أحد إجراءات التحقيق بشكل خاص، فضلا عن تحديد ماهية السلطات المعنية بإعطاء الإذن. أما فيما يتعلق بالمتطلبات الإجرائية، فقد أفادت أغلبية الدول أن هناك نطاقا واسعا من إجراءات التحقيق يمكن البدء بها على أساس "وجود دليل بشأن أحد أفعال الجريمة السيبرانية أو بلاغ بوقوع أحد أفعالها".[1] وتشترط الدول في أغلب الأحيان – نظرا لتدخل الإجراءات بدرجة عالية، مثل الوقت الحقيقي لجمع البيانات أو جمع محتوى البيانات – وجود أدلة على قيام جريمة سيبرانية جسيمة أو بلاغ بشأنها، أو متطلبات إجرائية مثل إثبات "السبب المحتمل" أو "الأسباب المناسبة" للاشتباه في وقوع أحد الجرائم.[2]

الشكل 5–12: المتطلبات القانونية لاستعمال إجراءات التحقيق

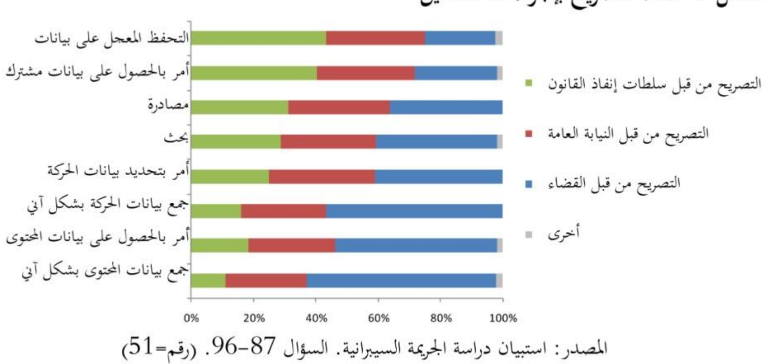


المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 87–96. (رقم=51)



وقد لوحظ وجود نمط مماثل فيما يتعلق بتحديد ماهية السلطات المنوط بها إصدار التصريح بشأن إجراءات التحقيق المختلفة. وفي هذا الصدد، أفادت الدول أنه في أغلب الأوقات تعتبر الإجراءات التدخلية قليلة إلى حد ما، مثل التحفظ المعجل على البيانات أو الأوامر الصادرة بشأن بيانات المشترك، ويمكن أن تصدرها سلطات إنفاذ القانون، بالمقارنة مع تدابير تدخلية بشكل أكبر.[3] فعلى سبيل المثال؛ ذكرت أكثر من نسبة 80 في المائة من الدول المجيبة أن الإجراءات التدخلية، مثل الأوامر المعنية بمحتوى البيانات أو الوقت الحقيقي لجمع البيانات، تتطلب إذنا من النيابة العامة أو إحدى المحاكم، أو بالأحرى مباشرة من الموظفين المكلفين بإنفاذ القانون. وبالرغم من ذلك؛ أفاد عدد قليل من الدول أن سلطات إنفاذ القانون لديها القدرة على إصدار الإذن لهذه التحقيقات، بيد أن ذلك يثير مخاوف إزاء كفاية الضمانات التي تستوعب

الشكل 5–13: التصريح بإجراءات التحقيق



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 87–96. (رقم=51)

---

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 87–96

[2] المرجع السابق.

[3] المرجع السابق.

هذه الإجراءات. وأخيرا؛ أفادت – على سبيل المثال – إحدى دول الأمريكتين أن المحكمة العليا قضت بعدم دستورية المادة الواردة في قانونها الإجرائي والتي نصت على جواز الاعتراض بدون أمر قضائي في ظروف استثنائية.[1]

تقييم الضمانات من خلال منظور حقوق الإنسان

شددت السوابق القضائية المستوحاة من المحاكم والمجالس الدولية لحقوق الإنسان عَلَى أن الحماية الإجرائية تعتبر من الأمور الدَامِغة لاحترام الخصوصية في سياق تحقيقات سلطات إنفاذ القانون. ويوضح الجدول أدناه الحق الدولي الأساسي المتعلق بأحكام الخصوصية، فضلا عن قرارات حقوق الإنسان المتعلقة بالمسائل مثل عدم وجود تشريع معني بالإذن المتعلق بإجراءات التحقيق؛ الضمانات التشريعية، والاستخدام العملي لإجراءات التحقيق. بيد أنه حتى الآن؛ تصدى بشكل مباشر عدد قليل من القرارات الدولية المعنية بحقوق الإنسان للتحقيقات في الجريمة السيبرانية التي تضطلع بإجرائها سلطات إنفاذ القانون.[2]

ومع ذلك، قد يمثل أحد الأحكام الهامة الصادرة عن المحكمة الأوروبية لحقوق الإنسان التوازن بين الخصوصية والتحقيقات التي تضطلع بإجرائها سلطات إنفاذ القانون. وفي سياق جرائم المحتوى عبر الإنترنت التي يتورط فيها أحد القصر، فإن سلطات إنفاذ القانون قد تكون غير قادرة على الحصول على بيانات المشترك من مقدم خدمة الإنترنت نظرا لحماية السرية الواردة في قانون الاتصالات السلكية واللاسلكية. وقد قضت المحكمة في هذا الصدد، بأن ذلك يعيق اتخاذ خطوة فعالة لتحديد الجاني وملاحقته قضائيا.[3]

بالرغم من أن حرية التعبير وسرية المراسلات تعتبر من قبيل الاعتبارات الأولية، كما يجب أن يُمنح مستعملو الاتصالات السلكية واللاسلكية وخدمات الإنترنت ضمانا بأن خصوصيتهم وحرية تعبيرهم محل احترام، بيد أن هذه الضمانة لا يجوز أن تكون مطلقة، ويجب أن تخضع إلى سياق الأولويات المشروعة، مثل منع الفوضى والجريمة... حيث تكمن مهمة المشرع في هذا الصدد بتوفير إطار للتوفيق بين المطالبات المختلفة التي تَبَارَى للحماية في هذا السياق.

المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 02/2872

[1] المرجع السابق

[2] على سبيل المثال، بالرغم من أن الحكمة الأوروبية لحقوق الإنسان قد اعتبرت رقابة البريد الإلكترونية واستخدام الإنترنت في سياق العمل. أُنظر المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 00/62617. في هذه القضية، لجأت المحكمة إلى تطبيق اختبارات التحديد بشأن ما إذا كان هناك تدخل في الخصوصية و(كشفت عن ذلك) ما إذا كان التدخل طبقا للقانون.

[3] المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 02/2872

أحكام القانون الدولي لحقوق الإنسان
المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية، المادة 11 من الاتفاقية الأمريكية لحقوق الإنسان [لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته (العهد الدولي)]، [لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته (الاتفاقية الأوروبية)]، [لا يجوز أن يتعرض أحد لتدخل اعتباطي أو تعسفي في حياته الخاصة أو في شؤون أسرته أو منزله أو مراسلاته (الاتفاقية الأمريكية).
عدم وجود تشريع يجيز الإذن لإجراءات التحقيق
المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 79/8691 قضت المحكمة بأنه في حالة عدم وجود قواعد قانونية تتعلق بنطاق وممارسة السلطة التقديرية، عند غياب القواعد القانونية، فإن الممارسة الاخْتِيَارِيّة لسَدَّ الحاجَة من قبل مقدمي خدمة الاتصالات السلكية واللاسلكية لتسجيل أرقام الهواتف المتلفنة ومدة المخابرة التليفونية، بناء على طلب إلى الشرطة متى" كان ذلك يشكل أمرا جوهريا لتحقيقات الشرطة، بالإضافة إلى ما يتعلق بالجريمة الجسيمة" يعتبر ذلك مُنَافيا للحق في الخصوصية.
المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 99/74114 اعتراض رسائل جهاز الاستدعاء من قبل الموظفين المكلفين بإنفاذ القانون باستعمال "نسخة" من جهاز الاستدعاء الخاص بأحد المشتبه بهم في غياب القانون الذي ينظم اعتراض رسائل أجهزة الاستدعاء، فإن ذلك يعتبر مُتَعَارِضا للحق في الخصوصية. وقضت المحكمة بأنه يجب على القانون المحلي أن يتضمن حماية ضد التدخل التعسفي في الخصوصية.
الضمانات التشريعية لإجراءات التحقيق
الأمم المتحدة–اللجنة المعنية بحقوق الإنسان البلاغ CCPR/C/82/D/903/1999 لا يعتبر اعتراض وتسجيل حركة البيانات بناء على إذن كتابي من أحد قضاة التحقيق في سياق في إطار التحقيق القضائي الابْتِدَائِيّ بشأن تورط أحد الأفراد في إحدى الجماعات الإجرامية المنظمة، انتهاكا لحق الخصوصية. وأوضحت اللجنة أن التشريع الذي بموجبه يصدر الإذن يجب أن يَفْصِّل الظروف المحددة التي تجيز التدخل، واعتباره مناسبا وضروريا لتحقيق الأغراض المشروعة المتوخاة من مكافحة الجريمة.
المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 02/2872 عدم فعالية التحقيق الجنائي نظرا لغياب حكم قانوني صريح يجيز الكشف عن بيانات الاتصالات في حالة جرائم المحتوى عبر الإنترنت، تعتبر مُتَعَارِضة مع الالتزامات الثابتة للحق في الخصوصية. وقضت المحكمة بأن المجني عليه لم يحظ بحماية فعّالة.
المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 00/82540 تعتبر الأحكام الواردة في أحد القوانين الوطنية المعنية بتنظيم إجراءات المراقبة السرية مُغَايِرة للحق في الخصوصية، حيث أكدت المحكمة على أن القانون لم ينص على أي استعراض لتنفيذ الإجراءات من قِبَل هيئة خارجية أو من قِبَل أحد الموظفين من خارج الدائرة، بالإضافة إلى ذلك؛ لم ينص القانون على إجراءات منوط بها الحفاظ على سلامة الأدلة المتحصل عليها وكذلك سريتها، أو إجراءات تتعلق بحماية الأدلة من الإتلاف، والتَوْجِيه الكامل للمراقبة متروكة لأحد أعضاء السلطة التنفيذية، بدلا من هيئة مستقلة.
إجراءات التحقيق عَمَلِيّا
الحكم الصادر عن محكمة البلدان الأمريكية لحقوق الإنسان في 6 تموز/ يوليو 2009 (قضية إيتشر) يعتبر تسجيل الدولة للمحادثات الهاتفية، ونشرها في وقت لاحق دون الاحترام الكامل للمتطلبات القانونية الوطنية مُتَضَادّا للحق في الخصوصية. وقد أكدت المحكمة أن طلب المراقبة لم يرتبط بأحد تحقيقات الشرطة أو الإجراءات الجنائية. وأوضحت المحكمة أيضا أن الاعتراض المصرح به وفقا لأحد التفسيرات القضائية فحسب لا يرتبط بالمنطقية أو الشروط الإجرائية أو الفترة الزمنية للإجراء.
المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 88/13710 يعتبر تفتيش أحد مكاتب المحامين بموجب إذن قضائي للتفتيش عن "وثائق" ومصادرتها من قبيل التعدي على سرية المهنة، علاوة على تعارض الإجراء مع الحق في الخصوصية. وقضت المحكمة أن الإجراءات تجاوزت الهدف منها.

وهناك عدد من القرارات الأخرى التي تعتبر أيضا ذات الصلة بشكل خاص بسياق التحقيق في الجريمة السيبرانية. ففي النظام الأوروبي؛ على سبيل المثال، يعتبر الدعم التَطَوّعِيّ لسجلات الهواتف من قبل مقدمي خدمة الاتصالات السلكية واللاسلكية من قبيل الأمور التي تتعارض مع الحق في الخصوصية في ظل غياب قواعد قانونية محددة[1]. وعلى نحو مماثل؛ في الأمريكتين، فإن تسجيل المحادثات الهاتفية المصرح به وفقا لأحد التفسيرات القضائية فَحَسْب لا يرتبط بأحد التحقيقات القائمة؛ يعتبر انتهاكا للحق في الخصوصية.[2]

من المرجح تطبيق المبادئ المستوحاة من هذه القضايا في المستقبل على القضايا المعنية بالجريمة السيبرانية. فعلى سبيل المثال، يظهر البحث عن ملفات في أحد أنظمة الحاسوب أو المراقبة السرية للبريد الإلكتروني أو حركة بروتوكولات الإنترنت، متوازيات متقاربة مع التفتيش المادي التقليدي والتصنت على المكالمات. وتعتبر أفعال مقدمي خدمة الإنترنت المتمثلة في تسليم البيانات إلى سلطات إنفاذ القانون (سواء كان بموجب اتفاق تعاون غير رسمي، أو بموجب أمر قضائي، أو تكليف بالحضور أو أي من الأوامر القانونية الأخرى) مُكَافِئة لتلك التي يضطلع بها مقدمو خدمة الاتصالات السلكية واللاسلكية. وبشكل خاص، فإن أرجحية وصول التحقيقات في الجريمة السيبرانية إلى مجموعة كبيرة من المعلومات الشخصية، ومنها رسائل البريد الإلكتروني، محادثات بروتوكول الاتصال الصوتي الثنائي الاتجاه عبر الانترنت، تواريخ تصفح الإنترنت، الصور الفوتوغرافية، يمثل مستوى عاليا من التدخل المحتمل بشكل خاص. ففي العديد من القضايا؛ مثل طلب تسجيلات من أحد مقدمي خدمة الإنترنت أو الوقت الحقيقي لجمع البيانات بشكل رسمي، وبالتالي ترتبط بالاجتهاد القضائي في مجال حقوق الإنسان بشأن المراقبة السرية،[3] بيد أن الشخص القائم بالتحقيق على الأرجح غافِل عن حقيقة متجسدة في التحقيق وطبيعة البيانات التي تم جمعها بالإضافة إلى نطاقها. وفي مثل هذه الظروف، وليس أقل منها، ونظرا للثغرات الناجمة عن سوء استخدام، فإن المحاكم الإقليمية لحقوق الإنسان حثت على الحذر بشكل خاص.[4]

وفيما يتعلق بنطاق الخصوصية ومناهج الضمان، أفادت الدول من خلال الاستبيان الملحق بهذه الدراسة، أن واقع مجموعة الحالات التي نظرتها المحاكم الدولية لحقوق الإنسان تظهر تَنَوّعا كبيرا في حماية الخصوصية أثناء التحقيقات التي تضطلع بإجرائها سلطات إنفاذ القانون. هذا، وسلطت القرارات الوطنيةالمتعلقة بالخصوصية – التي تم تناولها – مزيدا من الضوء على هذه النقطة. فعلى سبيل المثال فيما يتعلق بالقرارات الوطنية بشأن الإجراءات المعنية بوصول سلطات إنفاذ القانون إلى معلومات مشترك عن طريق أحد مقدمي خدمات الإنترنت؛ فإن مجموعة من هؤلاء يرون أن طلبات الشرطة من مقدمي خدمات الإنترنت لإمدادهم بمعلومات عن

---

[1] المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 79/8691

[2] الحكم الصادر عن محكمة البلدان الأمريكية لحقوق الإنسان في 6تموز/ يوليو 2009 (قضية إيتشر)

[3] بالإضافة إلى القضايا الواردة في الجدول، أُنظر أيضا المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 00/54934.

[4] في على سبيل المثال؛ قضت المحكمة الأوروبية لحقوق الإنسان بأن "صلاحيات المراقبة السرية للمواطنين، يوازي ما تفعله الدولة البوليسية، تعتبر مَقْبُولة بموجب الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية فقط بقدر الضرورة القصوى لحماية المؤسسات الديمقراطية. المحكمة الأوروبية لحقوق الإنسان، الالتماس رقم 95/28341.

أحد المشتركين بدون إذن قضائي يعتبر متوافقا مع التوقّعات التي ترد على الخصوصية التي يحظى بها العملاء، بيد أن آخرين يرون أن الإجراء القضائي المناسب يعتبر أمرا مطلوبا من قِبَل حقوق الخصوصية.[1]

وأخيرا؛ كما في سياق تقييم حقوق الإنسان للتجريم، فإن القانون الدولي لحقوق الإنسان يعتبر، إلى حد ما، مُؤهلا ليتسع لهذه الاختلافات من خلال المبادئ، مثل مبدأ هامش التقدير.[2] وبالرغم من ذلك؛ فمن الواضح أن الاتجاهات الوطنية المختلفة بشأن الخصوصية ستولد تحديات بشكل متزايد في سياق تحقيقات سلطات إنفاذ القانون عبر الحدود الإقليمية، إلى جانب تطورات مثل الحوسبة السحابية.

الخصوصية، الولاية القضائية، والحوسبة السحابية

تنطوي معالجة بيانات الحوسبة السحابية على بيانات متعددة بالمواقع أو بيانات المراكز، والموزعة عبر ولايات قضائية وطنية مختلفة، مع وحدات مختلفة للتحكم في البيانات الخاصة ومعالجتها.[3] وبالرغم من أن موقع البيانات قابل للمعرفة بشكل تقني، إلا أن مستخدمي الحوسبة السحابية في ظل الظروف الحالية لا يُبلغون دائما بمكان وجود بياناتهم. وتعتبر الاتجاهات القضائية بدورها لكل من نظام حماية البيانات التي تدير البيانات الموجودة من قبل مقدمي خدمة الحوسبة السحابية، وقانون الإجراءات الجنائية الذي يحكم تحقيقات سلطات إنفاذ القانون الوطنية من الأمور المتشابكة.[4]

وهذا يقدّم درجة عالية من الالْتِباس للمستخدمين بشأن نظام الخصوصية الذي سيسري على بياناتهم، إلى جانب ماهية الظروف التي تتيح انتهاك الخصوصية لأغراض تحقيقات هيئات إنفاذ القانون أو المراقبة الأمنية. وفي هذا الصدد، فإن التشريعات في بعض الدول، على سبيل المثال، تتضمن صلاحيات للمراقبة واسعة النطاق يجوز تطبيقها على البيانات التي تخص غير المواطنين والتي تعتبر "مُتَوَقّفة" في خوادم الحوسبة السحابية الواقعة في نطاق الولاية القضائية الوطنية.[5] وفي حالة تمييز ضمانات الخصوصية الوطنية بين المواطنين وغير المواطنين،[6] فإن المستخدمين: (1) قد لا يكونوا على دراية بهذه الإجراءات، و(2) لا يوجد مَلْجَأ قانوني، إما بموجب قانون الدولة التي تطبق هذه الإجراءات التحقيقية أو – يعتمد على التطبيق المكاني لقوانينهم الوطنية (والدَمْج القانوني لكِيَان مقدم خدمة الحوسبة السحابية) – داخل أوطانهم.

[1] See for example, *R v Ward*, 2012 ONCA 660 and *State v. Reid*, 194 N.J. 376 (2008).

[2] Legg, A., 2012. *The Margin of Appreciation in International Human Rights Law*. Oxford: Oxford Monographs in International Law.

[3] مفاهيم أخرى "لوحدات التحكم في البيانات ومعالجتها"، انظر التوجيه رقم 95/46/EC الصادر عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي في 24 تشرين الأول/أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات (بصيغته المعدلة بموجب اللائحة (مجلس أوروبا) رقم 2003/1882 الصادر من البرلمان الأوروبي ومجلس أوروبا في 29 أيلول 2003).

[4] أنظر على سبيل المثال؛ الإدارة العامة للسياسات الداخلية بالبرلمان الأوروبي، حقوق المواطنين والشؤون الدستورية 2012. مكافحة جرائم الإنترنت وحماية الخصوصية في الحوسبة السحابية.

[5] المرجع السابق.

[6] See for example, *Verdugo-Urquidez* 494 U.S. 259 (1990) and USFISCR No. 08-01

وقد أفادت الدول المجيبة على الاستبيان الخاص بهذه الدراسة بوجود اختلافات في الخصوصية التي تتناولها الولاية القضائية للقانون، كما أفادت أيضا بوجود مجموعة من الأحكام القانونية تتعلق بتطبيق حماية الخصوصية الوطنية خارج نطاق الحدود الإقليمية. فمن الملاحظ في المقام، أن عددا قليلا من الدول ذكرت أن حماية الخصوصية لديها تأثير خارج الحدود الوطنية، ومنها؛ تلك التي تخضع لشروط ما إذا كان الفعل أو الممارسة منحدرا من خارج الإقليم، بالرغم من وجود "روابط تنظيمية" مع إحدى هذه الدول. هذا، وأكدت دول أخرى أن القوانين الوطنية المعنية بالخصوصية لا تسري على البيانات الحاسوبية أو المراسلات الإلكترونية، إما في الوقت الحقيقي لجمعها أو المخزنة خارج الإقليم. في حين ذكرت إحدى الدول أن ذلك يعتبر بمثابة "سؤال مفتوح" بشأن ما إذا كانت تحظى المواد الحاسوبية الواقعة خارج البلاد بنفس الحماية المقررة [للخصوصية] باعتبارها مواد حاسوبية موجودة في أحد الخوادم [داخل الإقليم].[1] بالرغم من ذلك؛ فإن أغلبية الدول المجيبة قد أوضحت أن الحماية الوطنية للخصوصية تسري على إجراءات التحقيق الذي تم الاضطلاع به داخل الإقليم بناء على طلب إحدى سلطات إنفاذ القانون الأجنبية. كما أن إحدى الدول لاحظت، على سبيل المثال، أنه "عندما يقدم طلب للمساعدة القانونية المتبادلة من قِبَل دولة أجنبية يعتبر دخيلا على القانون المحلي الذي يحمي الخصوصية، فإن هذا الطلب يمكن استبعاده.[2]

يبيّن أحد الأعمال الأخيرة للبرلمان الأوروبي أنه *"في مجال الجريمة السيبرانية، فإن تحدي الخصوصية "في سياق الحوسبة السحابية يعتبر ذا أهمية أقل إذا لم يتم تجاهلها"*.[3] وبينما قد قامت الدول بتطوير مجموعة من ضمانات الخصوصية لإجراءات إنفاذ القانون ضمن سياق وطني، إلا أن ذلك يعتبر مُتَعَدّدا إلى جانب عدم سهولة توافقه في حالات التحقيق في الجريمة السيبرانية عبر الحدود الوطنية، ورُبّمَا يقود إلى تنازع القوانين أو ثغرات في الولاية القضائية. ومن الملاحظ في هذا الصدد؛ أن الدول تعمل على سن قوانين للتصدي إلى التوازن الدَقِيق بين الخصوصية الفردية ومنع الجريمة ومكافحتها، بيد أنه من الأهمية بمكان أن تعكس القوانين الوطنية المبادئ العامة لسيادة القانون وحقوق الإنسان لإجراءات التحقيق التي تضطلع بإجرائها هيئات إنفاذ القانون.

توضح إحدى نقاط البدء القوية الواردة في فقه حقوق الإنسان والتي تمت مناقشتها أعلاه وأُوجِزَت في الجدول أدناه، ماهية مبادئ سيادة القانون لقوانين المراقبة. ومع ذلك، فإن مثل هذه المبادئ لم تصطدم حتى الآن بالتحديات المعنية بقضايا نقل البيانات عبر الحدود الإقليمية. وفي هذا الصدد؛ بينما تعمل مواءمة معايير الخصوصية على المساعدة على زيادة إمكانية توقّع وصول هيئات إنفاذ القانون إلى مستخدم البيانات، بما في ذلك السلطات الأجنبية، فإن الدول أيضا ستحتاج للتصدي بشكل متزايد لنِطَاق الولاية القضائية للحماية الوطنية للخصوصية. وقد يتطلب ذلك كلّا من: (1) ضمان أن دعم التحقيقات التي تجريها سلطات إنفاذ القانون

---

[1] الاستبيان الخاص بهذه الدراسة، السؤال رقم 21.

[2] المرجع السابق.

[3] الإدارة العامة للسياسات الداخلية بالبرلمان الأوروبي، حقوق المواطنين والشؤون الدستورية 2012. مكافحة جرائم الإنترنت وحماية الخصوصية في الحوسبة السحابية

الأجنبية تخضع بشكل كامل إلى المعايير الوطنية للخصوصية، و(2) اعتبار أسباب الإجراء متاحة للأشخاص خارج نطاق الولاية القضائية الوطنية، والتي قد تأثرت بالإجراءات التي اتخذتها سلطات إنفاذ القانون للتلك الدولة.

قوانين المراقبة ومبادئ سيادة القانون

- يجب أن يكون القانون واضحا ليعطي مؤشرا كافيا للأوضاع والظروف عندما تُخَوّل السلطات في استعمال أحد إجراءات التحقيق، بما في ذلك:
    - طبيعة الجرائم التي تستدعي استعمال الإجراء
    - تحديد ماهية فئات الناس المعرضة لهذا الإجراء
    - حدّ الفترة الزمنية للإجراء
    - الإجراءات التي يتعين اتباعها عند فحص واستخدام وتخزين البيانات المتحصل عليها
    - الاحتياطات التي يتعين اتخاذها عند نَقْل البيانات إلى أطراف أخرى
    - ماهية الظروف التي يجب محو أو تدمير البيانات المتحَصَّل عليها أو يجوز فيها أداء ذلك
- الضمانات الكافية والفعالة التي يجب وجودها لمواجهة إساءة الاستخدام، مع الأخذ في الاعتبار ما يلي:
    - طبيعة ونطاق الإجراءات المحتملة والمدة الزمنية التي ستستغرقها
    - الأسباب المطلوبة لإصدار الأمر في مواجهتها
    - السلطة المختصة بالإجازة والتنفيذ والإشراف عليها
    - التدابير المنصوص عليها في القانون الوطني
- يتعين أن ينص القانون على قيام إحدى الهيئات أو الموظفين باستعراض تنفيذ الإجراءات إلى جانب الإشراف عليها، مع مراعاة أن تكون الهيئة أو الموظف المكلف بالاستعراض والإشراف إما من خارج نطاق خدمات نشر هذا الإجراء أو لديه مؤهلات مؤكدة تكفل استقلالها
- يجب أن ينص القانون على أنه بمجرد عمل الإخطار بدون المساس بالغرض من الإجراء عقب انتهاء العمل به، ينبغي تقديم المعلومات للأشخاص المعنية

ECtHR Application No. 62540/00

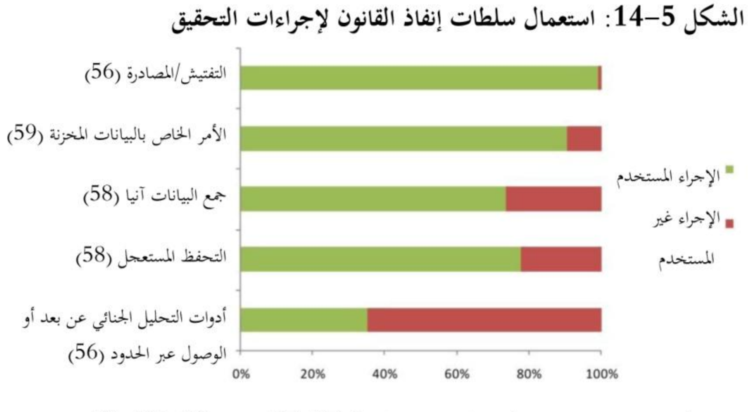
4-5 استعمال إجراءات التحقيق عمليا

الاستنتاجات الرئيسية

- بغض النظر عن الشكل القانوني لصلاحيات التحقيق، فإن كافة الدول تستعمل التفتيش والمصادرة للاسْتِيلاء المادي على جهاز الحاسوب وأخذ البيانات الحاسوبية
- تستعمل أيضا غالبية الدول أوامر قضائية للحصول على البيانات الحاسوبية من مقدمي خدمة الإنترنت، والوقت الحقيقي لجمع البيانات، والتحفظ المعجل على البيانات
- تواجه سلطات إنفاذ القانون مجموعة من التحديات في الممارسة العملية، منها التقنيات التي يستعملها الجناة لإخفاء أو حذف البيانات الحاسوبية ذات الصلة بإحدى الجرائم

بغض النظر عن الشكل القانوني للصلاحيات الممنوحة، فقد أشارت سلطات إنفاذ القانون المجيبة على الاستبيان الخاص بهذه الدراسة أن نِطَاق تدابير التحقيق –من التفتيش والمصادرة، إلى التحفظ المعجل على البيانات – تعتبر مستخدمة بشكل واسع من الناحية العملية. فعلى سبيل المثال؛ أفادت جميع الدول تقريبا باستخدام التفتيش والمصادرة للاسْتِيلاء المادي على جهاز الحاسوب وضبط البيانات الحاسوبية. علاوة على ما تقدم، فقد أفاد أيضا الضباط المكلفون بإنفاذ القانون (المجيبون على الاستبيان) بأن ما يزيد عن نسبة 90 في المائة من الدول تستعمل الأوامر في الحصول على البيانات الحاسوبية المخزنة، بيد أن ما يقرب من نسبة 80 في المائة من الدول المجيبة أفادت باستعمالها أوامر التحفظ المعجل على البيانات الحاسوبية.[1] وبالتزامن مع النسبة المنخفضة من الدول التي أفادت عن الصلاحيات القانونية ذات الصلة، فإن ما يقل عن نسبة 40 في المائة من الدول أدلت باستعمالها أساليب التحليل الجنائي عن بُعد أو الوصول "عبر الحدود الإقليمية".[2]

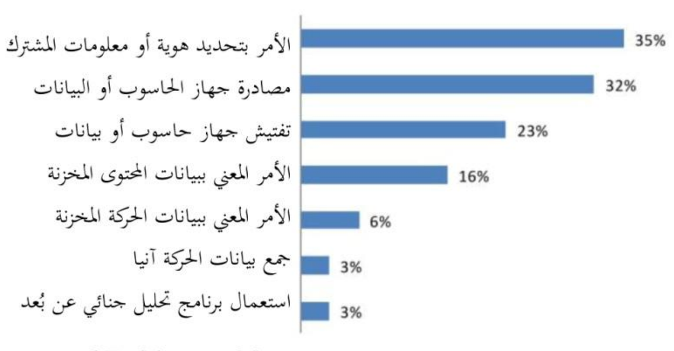
الشكل 5–14: استعمال سلطات إنفاذ القانون لإجراءات التحقيق



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 87–97. (رقم=56، 59، 58)

بينما تتناسب هذه الردود بشكل عام مع الصلاحيات القانونية التي أفادت الدول المجيبة بوجودها، إلا أن الأمر المعني بالتحفظ المعجل على البيانات الحاسوبية قد استخدم عمليا بشكل أكْثَر تكرارا إلى حد ما من الردود التي أفادت بوجود صلاحيات قانونية.[3] مما قد يعتبر ذلك ذا دَلَالَة بالتحفظ المعجل على البيانات بشكل عملي من خلال علاقات العمل غير الرسمية بين سلطات إنفاذ القانون ومقدمي الخدمات.

الشكل 5–15: إجراءات التحقيق الأكثر استخداما



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 98. (رقم=31، 37)

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 87–96.

[2] الاستبيان الخاص بالدراسة، السؤال رقم 87–96.

[3] أنظر أعلاه، القسم 5–2 لمحة عامة لصلاحيات التحقيق.

وقد أوضحت الدول المجيبة أيضا بشأن صلاحيات التحقيق *الأكثر استعمالا* ، أهمية التفتيش والمصادرة، فضلا عن استعمال الأوامر المعنية بالحصول على بيانات عن أحد المشتركين من مقدمي الخدمة. وفي ظل الزيادة الكبيرة للأجهزة المتصلة بالإنترنت، فإن البيانات الحاسوبية التي قد سبق وتم تخزينها فقط في أحد أجهزة الحاسوب المحلية تعتبر معالجة بشكل متزايد من قبل مقدمي خدمات القطاع الخاص، بما في ذلك خدمات الحوسبة السحابية. هذا، وقد عكست أهمية حصول الموظفين المكلفين بإنفاذ القانون على الأدلة الإلكترونية من مقدمي الخدمة، حقيقة أن الأوامر القضائية للحصول على معلومات بشأن أحد المشتركين تعتبر من أكثر الإجراءات المستخدمة في التحقيق، حسبما أفادت الدول بذلك. ويتناول القسم التالي المعني بالتحقيقات والقطاع الخاص، التفاعلات بين سلطات إنفاذ القانون ومقدمي الخدمات، بمزيد من التفصيل.

التحديات التي تواجه التحقيق والممارسة السليمة

حددت الدول المجيبة، على الاستبيان الخاص بهذه الدراسة، عددا من التحديات والممارسات السليمة ذات الصلة باستخدام إجراءات التحقيق والتحقيقات في الجريمة السيبرانية بشكل عام. وفيما يتعلق بالممارسة الجيدة، فقد أبرزت الدول أهمية التنظيم الدقيق وترتيب وتنسيق التحقيقات. فعلى سبيل المثال؛ أفادت إحدى الدول بأن "التحفظ على البيانات ومصادرة البيانات المخزنة والبيانات الحاسوبية بشكل سليم يتفق مع أساليب التحليل الجنائي يعتبر أحد أسس نجاح التحقيقات في الجريمة السيبرانية".[1] وفي هذا الصدد أيضا، ذكرت دولة أخرى أنه "يتعين تسجيل كافة الإجراءات وإفراغها في سجل قابل للمراجعة، إلى جانب ذلك، يتعين أن يكون كل إجراء وموقع إلكتروني وعنوان البريد الإلكتروني مؤرخا وموقوتا، مع تسجيل مصادر المعلومات والاتصالات".[2] بالإضافة إلى ذلك؛ فقد ذكر عدد من الدول بأن نقطة البداية للتحقيقات الناجحة تتجسد في المعلومات فِي أغلب الأوقات، مثل عناوين برتوكولات الإنترنت. وبالتالي، تتمثل الممارسة السليمة في التركيز على ضمان اسْتِطاعَة الحصول على المعلومات عن أحد المشتركين في الوقت المناسب.[3]

أما فيما يتعلق بالتحديات التي واجهت التحقيق، فإن العديد من الدول المجيبة أدلت بملاحظاتها بشأن التحقيقات التي تضطلع بإجرائها هيئات إنفاذ القانون، وذلك من خلال تسليط الضوء على مستوى تصاعد تطور الأعمال الإجرامية، مع ضرورة تتبع تحقيقات هيئات إنفاذ القانون مرتكبي الجريمة السيبرانية. فعلى سبيل المثال في هذا الشأن، ذكرت إحدى الدول الأوروبية أن *"الهجمات أصبحت أكثر فأكثر تقدما، علاوة على أن الكشف عنها أصبح أيضا أكثر فأكثر صعوبة، وفي نفس الوقت؛ فإن التقنيات تجد بشكل سريع طريقها نحو جُمْهُور أوسع، وقد لاحظنا أيضا أن المقَوّمات الرقمية (باعتبارها وسائل أو مسرحا للجريمة أو هدفا لها) أصبحت*

[1] الاستبيان الخاص بالدراسة، السؤال رقم 99

[2] المرجع السابق.

[3] المرجع السابق

أكثر فأكثر أهمية في ارتكاب كل الجرائم بشكل أساسي" .[1] هذا، وقد أكدت دولة أخرى على أن *"زيادة وُقُوع جرائم الإنترنت يعتبر مسيرا من قِبَل تَقَدّم الأدوات التقنية والبرنامجية المتاحة للجناة المدْعُومين بسوق غير مشروع لتسويق أدوات تستخدم في ارتكاب الجريمة السيبرانية"* .[2]

فمن الملاحظ أن تصاعد مستويات التَطْوِير يرافقه زيادة التحديات في مجالات، مثل: تحديد مكان الأدلة الإلكترونية، واستخدام الجناة تقنيات للتشويش، ومجابهة أحجام كبيرة من البيانات لتحليلها، بالإضافة إلى التحديات التي تصاحب الحصول على بيانات من مقدمي الخدمات. فعلى مستوى التحقيق الأساسي، تعتبر الارتباطية الرقمية والتخزين الرقمي مُنْدَمِجة مع الأدوات المنزلية والأغراض الشخصية المألُوفة، مثل؛ الأقلام الكاميرات والساعات ذات الذاكرة الوميضية، ومشغل الذاكرة الوميضية للناقل التسلسلي العالمي في شكل حِلى. بالإضافة إلى ذلك؛ أجهزة التخزين اللاسلكية التي يمكن إخفاؤها في تجاويف الحائط والأسقف والمساحات الأرضية. وعلى النحو الذي لاحظته إحدى الدول، فإن "سهولة الإخفاء" المادي (والإلكتروني) للبيانات الحاسوبية يمكن أن يمثل صعوبات عند إجراء التحقيقات.[3] وفي هذا الشأن أيضا، أبرزت الدول إشكاليات تتعلق "بأجهزة مَحْو البيانات المخزنة". ففي حالة استعمال الجناة خدمات الاتصال عبر الإنترنت، مثل نقل الصوت باستخدام بروتوكول الإنترنت، قد تتدفق البيانات الحاسوبية بشكل مباشر من مستخدم إلى مستخدم (وليست من خلال خوادم مقدمي الخدمة)،[4] مما يعني ذلك إتاحة النسخ المحلية فقط من بيانات مُعَيّنة، مع الأخذ في الاعتبار تعرضها للحذف لاحقا. إلى جانب ذلك؛ فإن الجناة قد يستخدمون رسائل "النقاط الميتة" في مُسَوّدَة المجلدات لحسابات البريد الإلكتروني (يسمح بالاتصال بدون "إرسال" بريد إلكتروني)، جنبا إلى جنب مع استعمال الوحدات العامة المجانية لتقنية الاتصال اللاسلكي، أو الهاتف المحمول المدفوع مسبقا، أو بطاقات الائتمان. هذا، وأبرزت إحدى الدول، على سبيل المثال، التحديات المتمثلة في " تحديد موقع" الاتصال نظرا لتوافر كم كبير من وحدات الاتصال المجانية.[5] وقد أفادت أيضا العديد من الدول باستخدام الجناة لتقنيات التشويش والتشفير، وسوف يتناول الفصل السادس (العدالة الجنائية والأدلة الإلكترونية) هذه المسألة بمزيد من التفصيل.

وأخيرا، أفادت العديد من الدول أن التحديات الكبيرة تكمن في الحصول على معلومات من مقدمي الخدمة. فعلى سبيل المثال؛ أفادت إحدى دول الأمريكتين أن تقديم مقدمي خدمة الإنترنت معلومات عن أحد المشتركين بشكل تتطوعي قد أدى إلى ممارسة متناقضة عبر الدولة.[6] كما أفادت دول أخرى؛ "بأن مقدمي الخدمة

[1] الاستبيان الخاص بالدراسة، السؤال رقم 85.

[2] الاستبيان الخاص بالدراسة، السؤال رقم 84

[3] الاستبيان الخاص بالدراسة، السؤال رقم 87-96

[4] See, for example, http://blogs.skype.com/en/2012/07/what_does_skypes_architecture_do.html

[5] الاستبيان الخاص بالدراسة، السؤال رقم 87-96

[6] المرجع السابق

لا يضطلعون بتخزين البيانات الحاسوبية لمدة "طويلة كافية"، حيث تأخذ مسألة تقديم البيانات إلى الشرطة من قِبَل المشترك وقتا كبيرا".[1] وأضافت إحدى الدول الآسيوية في هذا الشأن؛ أن التحدي يتمثل في تخزين مقدمي الخدمة لـ "تفاصيل تسجيل غير دقيقة".[2] وسيتم تناول التفاعل بين سلطات إنفاذ القانون ومقدمي الخدمات سواء بشكل رسمي أو غير رسمي في القسم التالي من هذا الفصل.

5-5 التحقيقات والقطاع الخاص

الاستنتاجات الرئيسية:

- يُعدّ التفاعل بين سلطات إنفاذ القانون ومقدّمي خدمات الإنترنت علاقة معقّدة بصفة خاصة. ذلك أنَّ لدى مقدّمي الخدمات المعلومات الخاصة بالمشتركين والفواتير وبعض سجلات الاتصال ومعلومات عن المواقع، ومحتوى الاتصالات
- وتختلف الالتزامات القانونية الوطنية المتّبعة في القطاع الخاص بشأن الاحتفاظ بالبيانات وإفشائها اختلافا كبيرا حسب الدولة وأوساط الصناعة ونوع البيانات. وقد أبلغت البلدان في معظم الأحيان عن اللجوء إلى أوامر قضائية للحصول على أدلة من مقدّمي الخدمات
- يتمثل أكثر ما يطلبه مقدمو الخدمات للإبلاغ في عملية قانونية واجِبة للكشف عن بيانات العميل. ولذلك؛ فإن غالبية الدول المجيبة أفادت بأنها تلجأ إلى الأوامر القضائية للحصول على الأدلة الإلكترونية من مقدمي الخدمات
- قد تتمكّن سلطات إنفاذ القانون في بعض الحالات من الحصول مباشرة على البيانات، مما ييسر ذلك الشراكة غير الرسمية بين سلطات إنفاذ القانون ومقدمي الخدمة

الحصول على البيانات من مقدمي الخدمة

تقدم الردود التي أبدتها الدول المجيبة على الاستبيان الخاص بهذه الدراسة وكذلك القطاع الخاص، صورة مشوشة متشابكة بشأن التفاعلات بين سلطات إنفاذ القانون والقطاع الخاص. وتتسم هذه الصورة بما يلي: (1) اختلافات بين الدول في الصلاحيات القانونية الممنوحة لاستصدار أمر بالإفراج عن البيانات الحاسوبية بناء على طلب مقدمي الخدمة، (2) تبرز التحديات حَيْثُمَا يقيم مقدمو الخدمات خارج الحدود الإقليمية، و(3) اختلافات في السياسات التي ينتهجها القطاع الخاص، إلى جانب تباين درجات التعاون الرسمي وغير الرسمي بينه وبين سلطات إنفاذ القانون.

---

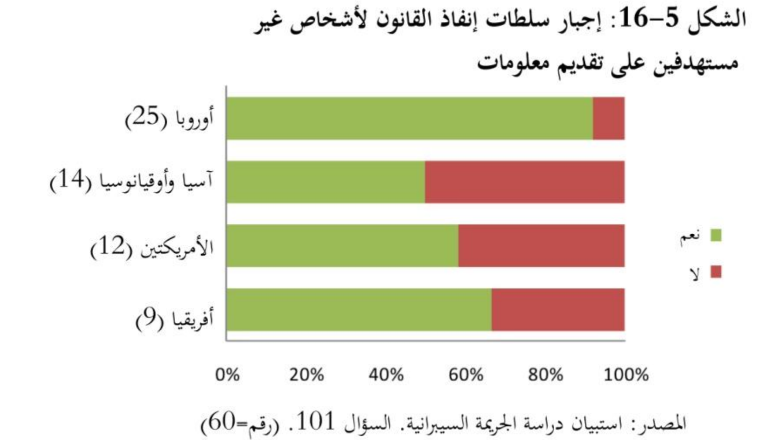
[1] المرجع السابق

[2] المرجع السابق

فمن المستقر، أن لدى مقدّمي الخدمات المعلومات الخاصة بالمشتركين والفواتير وبعض سجلات الاتصال ومعلومات عن المواقع (كبيانات أبراج الاتصالات اللاسلكية الخاصة بمقدّمي خدمات الهواتف الجوالة) ومحتوى الاتصالات؛ وقد تمثل كل هذه العناصر أدلّة إلكترونية مهمة عن جريمة معيّنة. ومع ذلك؛ فإن مقدمي الخدمة الإلكترونية بشكل عام غير ملتزمون بإبلاغ سلطات إنفاذ القانون بشكل تَأكِيدِيّ عن أي نشاط إجرامي يتم على شبكاتهم، (بالرغم من أنه في عِدّة دول، يعتبر استغلال الطفل في المواد الإباحية واجبا إلزاميّا يجب الإبلاغ عنه). وكنتيجة لذلك؛ تتجه الدول المجيبة نحو استعمال الصلاحيات القانونية للحصول على البيانات الحاسوبية من مقدمي الخدمة، وذلك في إطار المطلوب لأحد التحقيقات الجنائية. وكما ذكرنا آنفا؛ فقد أفادت غالبية الدول المجيبة بوجود صلاحيات عامة وصلاحيات خاصة بالفضاء السيبراني لاستصدار أمر بالحصول على البيانات من الأطراف الثلاثة، مثل مقدمي الخدمات.

هذا، وقد ذكرت على سبيل المثال الدول المجيبة، أنه "طبقا لقانون الإجراءات الجنائية، يجوز لأي شخص تَوْجِيه الإجراءات المأذون بها من قبل المدعي العام، عند الضرورة، لطلب التحفظ على البيانات التي قد ترتبط بجريمة مرتكبة".[1] وذكرت الدول أيضا؛ أنه "يجوز للشرطة أن تطلب من الأشخاص والشركات أن يدلوا بالشهادة باعتبارهم شهودا أو تسليم البيانات أو أداء أي شيء آخر من شأنه أن يساعد في القضية".[2] وبالرغم من ذلك؛ فإن تعليقات الدول المجيبة على الاستبيان أشارت إلى أن هناك عددا من الدول إما لا تزال تعاني من عدم كفاية الصلاحيات التشريعية أو تواجه تحديات بشكل عملي في الحصول على البيانات.[3] فمن الملاحظ أن الدول أفادت بمسألة مشتركة مفادها أن مقدمي خدمة الإنترنت يعتبرون غير مقيدين أحيانا كثيرة بأي التزام للاحتفاظ بالبيانات الحاسوبية، والتي بحلول الوقت قد صدر بشأنها الإذن بالأوامر اللازمة، في حين لم تعد سجلات الاتصال متاحة.[4] وأخيرا؛ أبرز أيضا عدد من الدول التحديات التي تثيرها مواجهة قضايا الخصوصية المتعلقة بتقديم البيانات من قِبَل مقدمي الخدمة.[5]

الشكل 5-16: إجبار سلطات إنفاذ القانون لأشخاص غير مستهدفين على تقديم معلومات



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 101. (رقم=60)

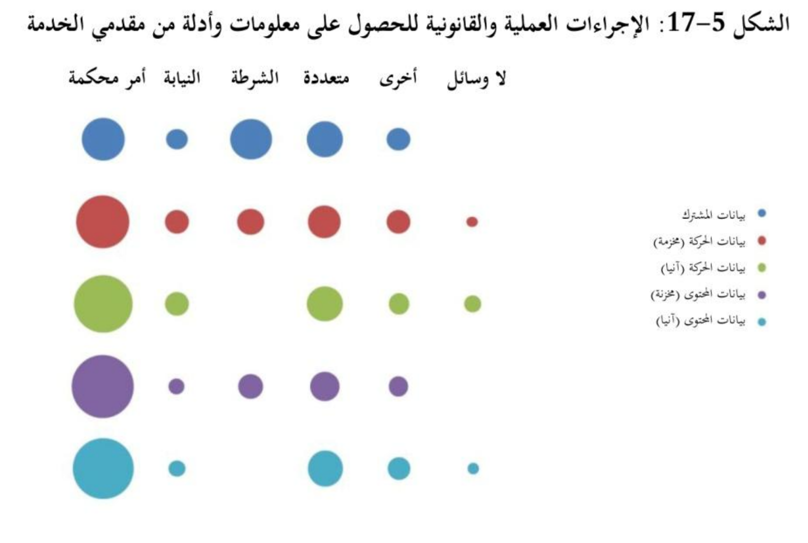
وقد أبلغت دول من خارج أوروبا بشكل متواتر عن هذه التحديات، يعتبر هذا النمط من

[1] الاستبيان الخاص بالدراسة، السؤال رقم 101
[2] المرجع السابق
[3] الاستبيان الخاص بالدراسة، السؤال رقم 89-91
[4] المرجع السابق
[5] المرجع السابق

التحديات مدعوما من قبل الردود التي أبدتها سلطات إنفاذ القانون بشأن التساؤل حول القدرة على إجبار أشخاص لا يستهدفهم التحقيق لتقديم معلومات. ويظهر الشكل 5–16 أن ما يقرب من نسبة 60 في المائة من الدول في أفريقيا وآسيا وأوقيانوسيا، والأمريكتين أكدت على إمكانية وجود ذلك. بيد أن كافة الدول الأوروبية تقريبا تفيد، من ناحية أخرى، بفعالية على أطراف ثالثة للحصول على المعلومات. تقدم هذه المعلومات سلطات إنفاذ القانون من منظور "عملي"، وذلك على النقيض من البيانات السابقة الواردة في هذا الفصل بشأن الصلاحية "القانونية" من حيث المبدأ.

أفاد أغلب الموظفين المكلفين بإنفاذ القانون باستخدامهم في الممارسة العملية الأوامر القضائية الرسمية بغية الحصول على بيانات حاسوبية من مقدمي الخدمة. ويوضح الشكل 5–17 التوزيع النسبي للاستجابات بشأن الأساليب المستخدمة للحصول على البيانات الخاصة بالمشتركين، وحركة البيانات المخزنة ومحتوى البيانات، بالإضافة إلى الوقت الحقيقي لحركة البيانات ومحتوي البيانات. وعلى النحو المتوقع من طبيعتها الأقل تدخلية، تعتبر الأساليب المستخدمة للحصول على بيانات المشتركين ذات طبيعة أكثر تنوعا، بما في ذلك الأوامر الصادرة من القضاء والنيابة العامة والشرطة.

الشكل 5–17: الإجراءات العملية والقانونية للحصول على معلومات وأدلة من مقدمي الخدمة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 102. (رقم=58)

وقد أفاد عدد من الدول أن هناك وسائل مُتَعَدّدة متاحة للحصول على البيانات، وهذا مُتَوَقّف على عدد من العوامل، تتضمن مرحلة التحقيق أو الإجراءات، والحاجة الملحة للطلب. وفي هذا الصدد، أفادت، على سبيل المثال، إحدى دول غرب آسيا أنه يمكن الحصول على محتوى البيانات المخزنة من أحد مقدمي الخدمة "بناء على أمر صادر من النائب العام أثناء عملية التحقيق، أو أمر يصدر من المحكمة أثناء إحدى مراحل المحاكمة.[1] وفي سياق الإطار ذاته، ذكرت دولة أخرى أن البيانات الخاصة بالمشتركين يمكن الحصول عليها بموجب "أمر من المدعي العام، أو في حالة الطوارئ؛ مذكرة من الشرطة بموافقة رسمية من المدعي العام.[2] هذا، وقد أُشير إلى الوسائل "الأخرى" المنوط بها الحصول على البيانات. ومن الملاحظ أن إحدى الدول، على سبيل المثال، سلطت الضوء على وسائل مُيَسّرة

[1] الاستبيان الخاص بالدراسة، السؤال رقم 102

[2] المرجع السابق

للحصول على البيانات الخاصة بالمشتركين، وذلك من خلال "الوصول إلى قاعدة بيانات الأرقام العامة الموَحّدة"، والتي تعتبر بمثابة قاعدة بيانات للمعلومات الخاصة بالمشتركين والتي تُرفع على حامل كبير يخضع للقانون.[1] وبشكل عام، فإن الردود أوضحت وجود تباين كبير في الوسائل التي تستخدمها الدول، ومنها؛ الاستدعاء من قِبَل الشرطة، الاستدعاءات "الرسمية"، والإشعارات القانونية، ومذكرات التفتيش، والأوامر القضائية، وأوامر التكليف بالحضور.

الحصول على بيانات من مقدمي الخدمة: مثال لإحدى التشريعات الوطنية لإحدى الدول في الأمريكتين

تنص إحدى التشريعات الفيدرالية في إحدى الدول من الأمريكتين على أنه يجوز لأي كيان حكومي بموجب مذكرة تفتيش فقط أن يطلب من قِبَل أحد مقدمي خدمة الاتصالات الإلكترونية الكشف عن محتويات أحد الرسائل الإلكترونية أو البرقيات التي تعتبر مخزنة إلكترونيا في أحد أنظمة الاتصالات الإلكترونية لمدة 108 يوم أو أقل. ويجوز، بموجب هذا القانون، لسلطات إنفاذ القانون المحلية الوصول إلى بعض أنواع البيانات والحصول عليها من خلال أمر استدعاء (صادر عادة من أحد المدعين العامين)، بشرط إصدار مذكرة تفتيش من إحدى المحاكم بغية الحصول على الأنواع الأخرى من البيانات.

إتصال بريد إلكتروني	إجراء التصريح
في التخزين عن بُعد، فتح	استدعاء
في التخزين عن بعد، غير مفتوح، ومخزن لمدة تزيد عن 180 يوم	
في الإرسال	مذكرة تفتيش
في التخزين في الحاسوب المنزلي	
في التخزين عن بعد، غير مفتوح، ومخزن لمدة تزيد عن 180 يوم أو أقل	

تتضمن أيضا التشريعات الوطنية أحكاما تلزم مقدم خدمة الإنترنت بالكشف عن مراسلات أحد العملاء في "الظروف الطارئة". وتجيز العديد من القوانين الوطنية لأحد الكيانات الوطنية الكشف عن محتوى وغير محتوى المراسلات، في حالة إذا كان مقدم الخدمة يعتقد بحسن نية أن حالة الطوارئ تنطوي على خطر الموت أو إصابة بدنية جسيمة لأي شخص مما يتطلب ذلك الكشف وبدون تأخير عن المراسلات ذات الصلة بحالة الطوارئ.

كما يجوز أيضا للموظفين المكلفين بإنفاذ القانون إصدار مذكرة إلى أحد مقدمي الخدمات بتكليفه بالتحفظ على السجلات والمواد الثبوتية الأخرى في حيازته لمدة تصل إلى 90 يوم لحين صدور أمر من إحدى المحاكم أو مذكرة حضور أخرى. في حالة عدم الامتثال إلى أحد هذه الأوامر، فإن ذلك يقْتَصَرَ على الجزاءات المدنية والغرامات ضد الشركة.

منظور القطاع الخاص

تضمن جمع المعلومات الخاصة بهذه الدراسة أيضا تجميع المعلومات من كيانات القطاع الخاص بشأن وجهة نظرها بشأن التعاون مع سلطات إنفاذ القانون، إلى جانب خبرتها في هذا المجال. وأفادت كيانات القطاع الخاص – التي أجابت على الاستبيان الخاص بهذه الدراسة – أن هناك مجموعة من السياسات الداخلية والالتزامات الخارجية متعلقة بطلبات سلطات إنفاذ قانون أجنبية ووطنية بشأن الحصول على بيانات. بالإضافة إلى

[1] المرجع السابق

أن العديد من سياسات القطاع الخاص تعتبر متاحة للجمهور في شكل "كتيبات إنفاذ القانون" والتي تقدم إرشادات توجيهية بشأن سياسات الإبقاء على البيانات وأطر طلبات سلطات إنفاذ القانون.[1]

في مستعرض الرد على الاستبيان الخاص بهذه الدارسة، أبْرزت سلطات إنفاذ القانون تحديات تتعلق بقصر المدة الزمنية للاحتفاظ بالبيانات من قِبَل كيانات القطاع الخاص ومقدمي الخدمة.[2] وفيما يتعلق بتوفير معلومات بشأن ممارسة الاحتفاظ بالبيانات، يقدم الجدول أدناه معلومات من إحدى عينات احتفاظ القطاع الخاص بالبيانات وسياسات وصول هيئات إنفاذ القانون. ويُبيّن الجدول أن نطاق البيانات يتم توليده وتخزينه أثناء تقديم خدمات الحوسبة والاتصالات الإلكترونية، كما يظهر أيضا السياسات المختلفة للاحتفاظ بالبيانات لهذه الأنماط المتباينة من البيانات، مما يعطى مؤشرا قويا للتحديات التي تواجهها سلطات إنفاذ القانون وكيانات القطاع الخاص في تحديد المعلومات المستخدمة في الأدلة والتأمين المناسب لها. هذا، ولا يضطلع مقدمو الخدمة بمراجعة المعلومات المتطابقة والمحْفُوظة لفترات زمنية مماثلة. وتراوحت فترة الاحتفاظ العلانية المتاحة ما بين أقل من يوم واحد إلى أجل غير مسمى، حيث إن بعض المعلومات ظهرت ليتم الاحتفاظ بها فقط أثناء الفترة الزمنية التي ظل فيها حساب المشترك نشطا وفعالا. وجدير بالذكر؛ أن عددا من كيانات القطاع الخاص أشارت إلى أن الاستجابة إلى طلبات سلطات إنفاذ القانون يمكن أن يكون بمثابة استهلاك للوقت، فتنفيذ هذه الطلبات لا يتم دائما بِيُسْر، ويرجع ذلك إلى برتوكولات وسياسات التخزين والتسجيل والاحتفاظ. وأخيرا، فإن توافر عدد كاف من الموظفين للرد على الطلبات قد يشكل عائقا أمام الامتثال أو ديمومته. أما فيما يتعلق بكيانات القطاع الخاص الأصغر، فإن الامتثال إلى طلبات سلطات إنفاذ القانون قد يبدو لهم أكثر عبئا من حيث نفقات العاملين والموارد.[3]

تخزين البيانات والاحتفاظ بها من قبل منظمات القطاع الخاص

الشركة	نوع البيانات المُنتجة	الفترة الزمنية للاحتفاظ بالبيانات	شروط الطلب الرسمي للكشف
مقدم خدمات الاتصال والمعلومات #1	محادثات غرف الدردشة	لا يوجد	
	محادثات الرسائل الفورية		
	سجلات دليل الأعضاء		
	سجلات الاتصال/بروتوكول الإنترنت		

[1] أنظر على سبيل المثال الرابط التالي:
https://www.facebook.com/safety/groups/law/guidelines/ ; http://pages.ebay.com/securitycenter/LawEnforcementCenter.html ; http://support.twitter.com/articles/41949-guidelines-for-law-enforcement# ; and http://myspace.desk.com/customer/portal/articles/526170-law-enforcement-support

[2] أنظر الفصل الثامن (المنع) القسم 8-3 مكافحة الجرية السيبرانية، القطاع الخاص والأوساط الأكاديمية، مكافحة الجريمة السيبرانية من قِبَل مقدمي خدمة الإنترنت ومقدمي خدمة استضافة المواقع.

[3] المقابلات التي تمت بشأن دراسة الجريمة السيبرانية (القطاع الخاص).

	للبريد الإلكتروني	60 يوم	نعم
	سجلات مجموعة بروتوكولات الإنترنت		
	سجلات الوصول إلى الاتصال بالإنترنت		
	سجلات اتصال (الهواتف المتلفزة) ANI		
مقدم خدمات اتصال ومعلومات #2	سجلات تواريخ اتصال بروتوكولات الإنترنت	60 يوم	نعم
	البيانات الخاصة بالمعاملات التجارية	90يوم (خاص)/60 يوم (مجموعات)	
	سجلات تسجيل حساب البريد الالكتروني	طوال فترة وجود الحساب	
	حساب الألعاب الإلكترونية		
	سجلات بطاقات الهوية		
خدمات اتصال ومعلومات #3	معلومات بشأن حساب مواقع البريد	فترات زمنية مختلفة للاحتفاظ	نعم
	سجل ملفات عناوين بروتوكولات الإنترنت	180 يوم	
	سجلات الحساب	سنتان بحد أدنى	
	سجلات تفاصيل المكالمات		
مقدم خدمات اتصال	الرسائل الفورية	30-90 يوم	نعم
	محتوى الرسائل المرئية (عبر الفيديو)		
	البريد الصوتي		
	المعاملات المالية	بقدر الضرورة	
	تسجيل البيانات		
	معلومات بشأن الخدمة والحساب		
مطوّر لعبة ومقدم شبكة #1	المراسلات الخاصة بالمستخدم	فترات زمنية مختلفة (تصل إلى 180 يوم)	نعم
	معلومات الحساب	إلى أجل غير مسمى	
	سجلات برتوكولات الإنترنت		
مقدم معلومات وخدمات #1	نطاقات	فترات زمنية مختلفة (من يوم إلى ما لا نهاية)	
	بريد الكتروني		
	سجلات اتصال برتوكولات الإنترنت للخوادم النائبة	5-7 أيام	نعم

	سجلات اتصال بروتوكولات الإنترنت للعضو	90 يوم	
	سجلات مصادر اتصال بروتوكولات الإنترنت		
	سجلات الدورة	6 أشهر	
مقدم معلومات وخدمات 2#	نطاقات/سجلات ومحتوى نشاط استضافة مواقع	30 يوم بحد أدنى بعد انتهاء المجموعة/الموقع الإلكتروني/النطاق	نعم
	سجل محتوى المجموعات والنشاط		
	محادثة نصية/سجلات الرسائل الفورية	45-60 يوم	
	بريد الكتروني	4 أشهر أو أكثر من عدم النشاط	
	معلومات مشترك	18 شهر بعد عدم النشاط	
	محتوى حساب	90 يوم بعد حذف الحساب	
	لمحات مختصرة		
	سجلات حساب عناوين بروتوكولات الإنترنت	تصل إلى سنة واحدة	
مقدم خدمة تراسل	معلومات المشترك	فترات احتفاظ مختلفة	نعم
	محتوى الحساب وصلات/روابط، ملفات تعريف الارتباط معلومات الموقع معلومات الدخول بيانات الويدجت	تصل إلى 37 يوما بعد حذف الحساب	
مقدم شبكة تواصل اجتماعي #1	بيانات تسجيل (معلومات أساسية للمستخدم المشترك)	تصل إلى 90 يوما بعد حذف الحساب	نعم
	بيانات عن المعاملات (سجلات بروتوكولات الإنترنت)		
مقدم شبكة تواصل اجتماعي #2	مراسلات المستخدم الخاصة	فترات زمنية مختلفة للاحتفاظ	نعم
	معلومات أساسية بشأن هوية المستخدم، سجلات عامة	بقدر بقاء الحساب/10 أيام بعد حذف الحساب	
	سجلات عناوين بروتوكولات الإنترنت	90 يوم	

اتضح أن الشاغل الرئيسي للشركات المعنية بطلبات سلطات إنفاذ القانون يتمثل في القدرة على تقديم البيانات عند طلبها، ولكن *"بدون التدخل في نطاق المتطلبات التشريعية أو التنظيمية الأخرى"*.[1] وفي هذا السياق، أشارت كيانات القطاع الخاص إلى شروط استعمال الخدمة من قِبَل العميل واعتبارات الخصوصية. وبالرغم من ذلك؛ فإن كيانات القطاع الخاص أبرزت بشكل خاص وجوب استجابتها بسرعة وبشكل إيجابي إذا كانت *"الحياة معرضة للخطر"*، ولكن لاحظت أيضا أن ذلك يحدث *"بشكل قليل جدا"*.[2] هذا، وتشتمل ردود كيانات القطاع الخاص على مقدمي الخدمة، ووضع تمييز واضح بين المتطلبات القانونية الرسمية لتقديم البيانات وبين الطلبات غير الرسمية. وأفادت تقريبا كافة الشركات المجيبة بأنه *"يجب"* علينا *"الاستجابة"* للأوامر الرسمية الصادرة عن المحاكم المحلية لتقديم معلومات *"طبقا للقوانين المعمول بها"*،[3] و*"متماشيا مع مسؤوليتنا القانونية"*.[4] *وفي هذا الصدد على سبيل المثال، فقد أفادت إحدى كيانات القطاع الخاص أنه عند ورود أحد الطلبات، فإن الخطوة الأولى تتمثل في تحديد "إذا كان هناك حق قانوني أساسي لطلب المعلومات أو يوجد التزام قانوني بالكشف عن المعلومات وتقديمها، مع الحرص على ضمان أننا لا ننتهك أيّا من القوانين الأخرى أو الالتزامات التعاقدية للشركة أمام العملاء، وخصوصيتهم"*.[5]

هذا، وقد أفادت غالبية كيانات القطاع الخاص بأنهم لا يعتبرون أنفسهم تحت وطأة أي التزام لتقديم بيانات استجابة لأحد الطلبات *"غير الرسمية"* – مثل المكالمة الهاتفية – الواردة من سلطات إنفاذ القانون. وبالرغم من أن عددا من كيانات القطاع الخاص قد أفادت بأنها قد تفضل تقديم بيانات بشكل تطوعي في استجابة منها للطلبات غير الرسمية طبقا لسياستها الداخلية الخاصة بها. فعلى سبيل المثال، ذكرت إحدى الشركات الدولية بأنها على استعداد للاستجابة لمثل هذه الطلبات *"إذا كانت البيانات متاحة ويتوافق تقديمها مع اللوائح القانونية للموارد البشرية بالشركة"*.[6] فمن الملاحظ أن عددا كبيرا من كيانات القطاع الخاص قد أفادت بأنها على استعداد للتجاوب مع الطلبات الرسمية لسلطات إنفاذ القانون بتقديم البيانات، مثل أحد المذكرات الرسمية. ومع ذلك، فجميع الكيانات تقريبا أشارت إلى أن ذلك لا يعتبر التزاما مطلقا، وأن مسألة تقديم البيانات مرهونة بشروط محددة، مثل إذا كان *"هناك التزام قانوني بتقديم معلومات والكشف عنها لا يشكل انتهاكا للقوانين الأخرى أو الالتزامات التعاقدية للشركة"*.[7]

[1] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 24

[2] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 26

[3] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 24-27

[4] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 24

[5] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 24-27

[6] المرجع السابق.

[7] المرجع السابق

فكثيرا ما أفادت الشركات الدولية ومقدمو الخدمة الوطنيون أن هيئات إنفاذ القانون تخصص وحدات اتصال بغية تيسير التعاون مع سلطات إنفاذ القانون، وتشتمل هذه الوحدات على: وحدات الاستجابة لحوادث الأمن السيبراني، وإدارة مخاطر وأمن وشرعية تكنولوجيا المعلومات أو وحدات تأمين تكنولوجيا المعلومات. بيد أن الشركات الأخرى لديها أفرقة متعددة التخصصات أو أفرقة عمل لإدارة العلاقات مع سلطات إنفاذ القانون. وقد أفادت بعض كيانات القطاع الخاص بأن آليات تعزيز التعاون وتبادل المعلومات مع سلطات إنفاذ القانون لا تزال في مَسَار التنمية.[1] وجدير بالذكر؛ أن هذه الآليات تعتبر من الأمور الهامة في ضوء تزايد عدد طلبات سلطات إنفاذ القانون بشأن تقديم البيانات من مقدمي الخدمة. فعلى سبيل المثال، أفاد أحد مشغلي الاتصالات السلكية واللاسلكية متعددة الجنسيات بأن هناك زيادة تقدر بـ 50 ضعفا في عدد الطلبات الرسمية الواردة بشأن البيانات الحاسوبية ما بين عامي 2008 و2010.[2]

وأبرزت أيضا كيانات القطاع الخاص حقيقة مؤداها أنها غالبا ما تتلقى طلبات من سلطات إنفاذ القانون الوطنية والأجنبية. إلى جانب ذلك؛ أفاد العديد من الشركات بأنها تنظر طلبات سلطات إنفاذ القانون الأجنبية الواردة فقط عبر "القنوات الرسمية" الوطنية.[3] هذا، وقد ذكرت بعض الشركات، على سبيل المثال، أنه يتعين على سلطات إنفاذ القانون الأجنبية الحصول على أمر بشأن البيانات من إحدى المحاكم الوطنية، وذلك من خلال طلب المساعدة القانونية المتبادلة. بالإضافة إلى ذلك؛ أفادت الشركات التي لديها مكاتب في دول مُتَعَدّدة بأن العمليات الوطنية المختلفة دائما في حاجة إلى مراعاة القوانين واللوائح المحلية. ومع ذلك؛ فإن كيانات القطاع الخاص متعددة الجنسيات حددت بشكل عام "مَقَر" الولاية القضائية الرئيسي لاستلام طلبات إنفاذ القانون على المستوى العالمي.[4]

بالإضافة إلى أحد المتطلبات العامة المعنية بالضمانات الإجرائية الواجبة "لمقر" الولاية القضائية لإحدى الشركات، فإن عددا من كيانات القطاع الخاص ذكرت أنه يتعين أن تمتثل الطلبات غير الرسمية لسلطات إنفاذ القانون الأجنبية إلى مَبْدَأ "السلطة التقديرية".[5] وتشير المعلومات المتاحة علانية لمقدمي الخدمة العالمية، مثل جوجل على سبيل المثال، إلى أن: "استعمال معاهدات المساعدة القانونية المتبادلة والإجراءات الدبلوماسية والتعاونية الأخرى، فإن الهيئات [الأجنبية] يمكنها العمل من خلال ["مقر" السلطات الوطنية] لجمع الأدلة الخاصة بالتحقيقات المشروعة"، وأنه على المستوى التَطَوّعِيّ، فإنه يمكننا تقديم بيانات أحد المستخدمين في استجابة منا للإجراءات القضائية الصحيحة لهيئات إنفاذ القانون [الأجنبية]، في حالة إذا كانت هذه الطلبات

---

[1] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 30
[2] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 35
[3] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 28
[4] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 28
[5] المرجع السابق

تعتبر متوافقة مع المعايير الدولية، والأسس الوطنية القانونية، وسياسات شركة جوجل، وقانون الدولة مقدمة الطلبة".[1]

وهذا يضيف إلى إحدى صور الشرط التكميلي لسلطات إنفاذ القانون الأجنبية للحصول على أوامر الاستدعاء الضرورية أو الأوامر القضائية أو الأوامر الصادرة في نطاق "مقر" الولاية القضائية لأحد مقدمي الخدمة، إلى جانب نطاق التَقْدِير المحدد لتقديم البيانات إلى سلطات إنفاذ القانون في إطار القيود الواردة في القوانين الوطنية وشروط استخدام الخدمة من قِبل العميل. ومن الملاحظ أن هذه العلاقات التقديرية بين القطاع الخاص وهيئات إنفاذ القانون تعتبر مُؤَسّسة بشكل واسع على الثقة وليس على افتراض الالتزام القانوني، ولذلك، عادة ما توجد هذه العلاقات ضمن مناطق جغرافية أو اجتماعية أو سياسية محدودة. هذا، وذكرت إحدى الشركات الكائنة في أمريكا الوسطى، على سبيل المثال، أنها قبلت الالتزامات المنبثقة من طلبات سلطات إنفاذ القانون، ولكن الامتثال يقتصر بالتحديد على الطلبات الواردة من السلطات المحلية. إلى جانب ذلك، فقد حددت إحدى الشركات الأوروبية بأنها تعاملت مع الطلبات غير الرسمية الواردة من سلطات إنفاذ القانون الأجنبية بنفس الطريقة التي تتعامل بها مع الطلبات الواردة من السلطات المحلية،[2] ولكنها لا تعتبر نفسها ملتزمة قانونيا بالامتثال إلى أي أسلوب أيا كان.[3] وعلى النحو الذي ذكرته إحدى الشركات الرائدة في توفير الخدمات عبر الإنترنت، "بأنها تعمل بحسن نية مع السلطات، ولكن ليس لدينا أي التزامات لأداء ذلك، وفي حالة انتهاك حسن النية، فإننا نفكر بِتَأَنٍّ أكثر في التعاون مع تلك السلطات".[4] وبعبارة أخرى؛ فإنه في حدود قوانين حماية البيانات، وشروط ومتطلبات استعمال الخدمة، فإن مقدمي الخدمة لديهم قدر كبير من حرية التصرف في البيانات التي تم الكشف عنها، بما في ذلك؛ هيئات إنفاذ القانون الأجنبية. وغني عن البيان؛ أن هذه القرارات غالبا ما تصدر على أساس وجود علاقات عمل وأواصر من الثقة. وفي هذا الصدد، فقد ذكرت إحدى الشركات الدولية العاملة في معدات الشبكات، على سبيل المثال، أن جميع الطلبات "تخضع للمراجعة" من أجل ضمان إمكانية التحقيق التقني والملاءمة مع شَرْعِيّة [...] لدولة معنية و[...] لوائح حقوق الإنسان.[5]

إن مزج: (1) القدرات المتباينة لسلطات إنفاذ القانون الأجنبية لكفالة الضمانات الإجرائية الواجبة في "نطاق" الولاية القضائية من خلال المساعدة القانونية المتبادلة، و(2) وجود شبكات اعْتِماد غير رسمية، يؤدي إلى تَغَايُر في نطاق الامتثال للطلبات الأجنبية للحصول على معلومات من الشركات الدولية المعنية بتقديم الخدمات. هذا، ويظهر الشكل 5-18 عددا من الطلبات الواردة من دول مختلفة وتَنفيذها (على النحو المدرج لكل

---

[1] See, for example, http://www.google.com/transparencyreport/userdatarequests/legalprocess/

[2] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 28

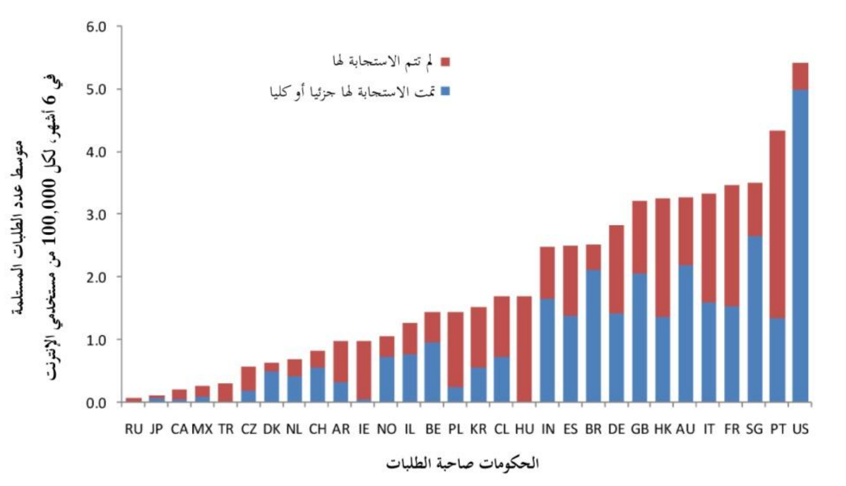
[3] المرجع السابق

[4] مجلس اللوردات ومجلس العموم. مشروع اللجنة المشتركة بشأن قانون بيانات الاتصال-التقرير الأول. المادة 6 (المسائل المتعلقة بالولاية القضائية-الطلبات الموجهة إلى مشاريع دعم المجتمعات المحلية في الخارج) 28 تشرين الثاني/نوفمبر 2012.

[5] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 28

100,000 مستخدم من مستخدمي الإنترنت في الدولة مقدمة الطلب) حسبما أفاد تقرير شركة جوجل بشأن الشفافية.[1] أما فيما يتعلق بالطلبات الواردة من الدول الأخرى، فقد تباينت ما بين صفر في المائة من الطلبات التي تم تنفيذها، إلى 80 في المائة تقريبا، بمتوسط قدره حوالي 80 في المائة من الطلبات التي تم تنفيذها. ومما لا شك فيه أن هذا النمط يُشتقّ على الأرجح من العديد من العوامل، بما في ذلك النطاق الذي تتم فيه طلبات سلطات إنفاذ القانون الأجنبية بشكل غير رسمي أو مباشرة، بالأحرى من خلال المساعدة القانونية المتبادلة، وسياسات الشركة تجاه الطلبات غير الرسمية من الدول المختلفة، واسْتِطاعَة السلطات الأجنبية على إعداد طلبات المساعدة القانونية المختلفة.


الشكل 5–18: طلبات بيانات المستخدمين التي تلقتها جوجل من حكومات (1 كانون الثاني/يناير 2011 – 30 حزيران/ يونيو 2012)



المصدر: عرض مكتب الأمم المتحدة المعني بالمخدرات والجريمة لبيانات تقرير جوجل للشفافية

يمكن تمديد نطاق العلاقات غير الرسمية بين سلطات إنفاذ القانون وكيانات القطاع الخاص بشكل أوسع من تقديم البيانات الحاسوبية لأغراض التحقيقات. وقد أفادت كل من الدول وكيانات القطاع الخاص، أثناء جمع المعلومات الخاصة بهذه الدراسة، بأن هناك مجموعة واسعة من مجالات التعاون. وفي هذا الصدد، أفادت إحدى دول شمال أوروبا، على سبيل المثال، أن "لدى سلطات إنفاذ القانون علاقة عمل غير رسمية مع مقدمي الخدمات الأسَاسِيّين لتحديث معلومات الاتصال ووضع إجراءات لتبادل البيانات بشكل رسمي".[2] في حين ذكرت دول أخرى، أن "هناك قواعد للممارسات التطوعية تسمح بتبادل المعلومات، جنبا إلى جنب مع التشريعات الرسمية".[3]

وباستقراء الواقع العملي، فقد أفادت عدة دول بتركيزها بشكل خاص على العلاقات مع شركات ومقدمي خدمات الاتصالات السلكية واللاسلكية. فعلى سبيل المثال، ألمحت إحدى الدول إلى أن "هيئات إنفاذ القانون تبقي على علاقات وَثِيقة مع شركات صناعة الاتصالات السلكية واللاسلكية، ولاسيما المشاركون في

---

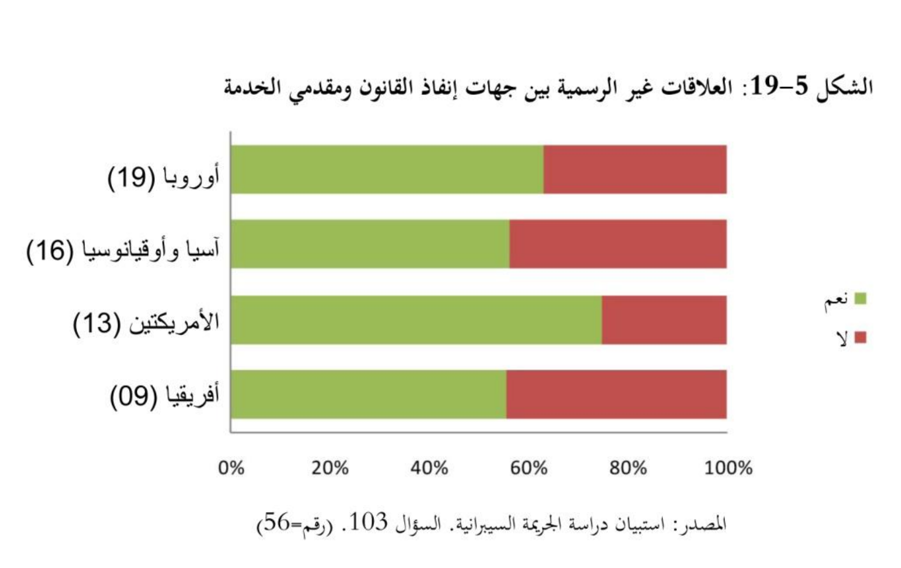
[1] See http://www.google.com/transparencyreport/userdatarequests/

[2] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 103

[3] المرجع السابق

الصناعات الضَخْمة". وتستمر هذه العلاقات في المقام الأول في مناقشة التدابير العملية (مثل ماهية أفضل الإجراءات المعنية بأوامر التبليغ، ونشر القدرات، وتقديم المعلومات التي تم اعتراضها بصورة قانونية)، والمسائل التقنية (مثل تشغيل شبكات الاتصالات السلكية واللاسلكية)، وقضايا السياسة العامة.[1] وتشير أيضا المعلومات المقدمة من كيانات القطاع الخاص إلى أن العديد من الشركات ترتبط بشراكات ليس فقط مع مقدمي الخدمة الإلكترونية، بل أيضا مع هيئات إنفاذ القانون. ويشتمل ذلك على أغراض تقَاسم المعلومات العامة بشأن تهديدات اتّجاهات الجريمة السيبرانية من أجل تيسير عمليات الإبلاغ عن حالات الاشتباه بوقع جريمة سيبرانية[2]. أما ما يتعلق بالشراكات بين القطاع العام والقطاع الخاص بشأن الجريمة السيبرانية، فقد تمت مناقشتها على نطاق أوسع في الفصل الثامن (المنع).

الشكل 5-19: العلاقات غير الرسمية بين جهات إنفاذ القانون ومقدمي الخدمة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 103. (رقم=56)

وتظهر ردود الدول على الاستبيان المرافق لهذه الدراسة أن العلاقات غير الرسمية بين هيئات إنفاذ القانون ومقدمي الخدمة تعتبر من الأمور المتعارف عليها في مختلف المناطق. ويوضح الشكل 5-19 أن بين نسبة 50 في المائة و60 في المائة من الدول في كافة المناطق قد أفادت بوجود مثل هذه العلاقات.[3]

أفاد عدد من الدول بشكل حَذِر أن العلاقات غير الرسمية بين هيئات إنفاذ القانون ومقدمي الخدمة تنطوي على تقاسم معلومات "لا تزج بالبيانات الخاصة بأحد العملاء".[4] ومع ذلك، فإن دولا أخرى تشير إلى أنه بدا لها أنه يمكنها تقديم البيانات الفردية لأحد العملاء إلى سلطات إنفاذ القانون من خلال هذه الاستعدادات.[5] بينما يمكن أن تساهم العلاقات الثابتة والفعّالة بين سلطات إنفاذ القانون ومقدمي الخدمة بشكل كبير في تقديم مساعدة فَعّالة للتحقيقات في الجريمة السيبرانية، فمن الأهمية بمكان أن تتفق هذه الترتيبات مع سيادة القانون والمعايير الدولية لحقوق الإنسان. وعلى النحو الذي تم استعراضه في هذا الفصل، فإن هذه الترتيبات يتعين أن

---

[1] المرجع السابق

[2] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال 40-45

[3] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 103

[4] أنظر أعلاه؛ القسم 3-5 إجراءات التحقيق والخصوصية، وجود حماية للخصوصية والضمانات الإجرائية

[5] See, for example, http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

تتضمن وضوحا كافيا بشأن الأوضاع والظروف التي يُعْهد بها إلى سلطات إنفاذ القانون للحصول على البيانات الحاسوبية، مع وضوح ماهية الضمانات الفعالة والملائمة ضد أي إساءة استعمال.[1] ومثال على غرار الترتيبات، فقد تخضع "محَطّة" وصول سلطات إنفاذ القانون إلى المشتركين غير المقيّدين أوحركة البيانات أو محتوى البيانات المخزنة من قبل مقدمي الخدمة إلى مستويات معينة من مراقبة حقوق الإنسان.[2]

6-5 قدرات سلطات إنفاذ القانون

الاستنتاجات الرئيسية:

- بدأ أكثر من 90 في المائة من البلدان التي أجابت عن الاستبيان بإنشاء هياكل متخصصة للتحقيق في الجريمة السيبرانية والجرائم التي تنطوي على أدلّة إلكترونية
- تفتقر هذه الهياكل في الدول النامية إلى ما يكفي من الموارد والقدرات
- لدى الدول الأقل نموّا عدد أقل بكثير من أفراد الشرطة المتخصصين، بمعدل يبلغ نحو 0.2 لكل 100,000 مستخدم إنترنت ضمن البلد المعني، في حين يكون هذا المعدّل أعلى بمرتين إلى خمس مرات في البلدان التي تفوقها تقدما
- 70 في المائة من الموظفين المتخصصين المكلفين بإنفاذ القوانين في الدول الأقل نموّا يفتقرون إلى المهارات والمعدات الحاسوبية

يتناول هذا القسم المعلومات التي تم جمعها بشأن قدرات سلطات إنفاذ القانون لمنع ومكافحة الجريمة السيبرانية، حيث تشتمل "القدرة" المؤسسية، في سياق حفظ الأمن والنظام العام، على عدد من العناصر، منها: القدرات التشغيلية والاستراتيجية، المهارات الفنية للموظفين، وكِفَايَة الضباط والموارد.[3] بيد أن هناك عنصرا آخر هامّا من عناصر القدرات يتمثل في مستوى "التَخَصّص". فالجرائم التي تقتضي ردا "متخصصا" تعتبر تلك التي تشكل تحديات من حيث تعاريف الجريمة، وتطبيق القانون، أو جمع الأدلة وتحليلها.[4] وتُظهر الجريمة السيبرانية كل هذه السمات، حيث يعتبر مستوى تخصص سلطات إنفاذ القانون من الأمور الحيوية لمكافحة أي جريمة بشكل فعال، إلى جانب الاستجابة للعدالة الجنائية. هذا ويمكن أن يجري تخصص سلطات إنفاذ القانون على كل من المستوى التنظيمي ومستوى شؤون الموظفين، فغالبا ما يتداخلان كلاهما معا. فبينما يعتبر التخصص من الأمور المتَوَقّع طلبها في مجال الجريمة السيبرانية والأدلة الإلكترونية، إلا أنه من المتوقع أيضا – مع تقدم العالم نحو زيادة

[1] الاستبيان الخاص بالدراسة (القطاع الخاص)، السؤال رقم 103

[2] المرجع السابق

[3] Katz, C.M., Maguire, E.R., Roncek, D.W., 2002. The Creation of Specialized Police Gang Units. *Policing,* 25(3):472-506

[4] Mace, R.R., 1999. *Prosecution Organizations and the Network of Computer Crime Control.* (Doctoral dissertation). AAT 9920188.

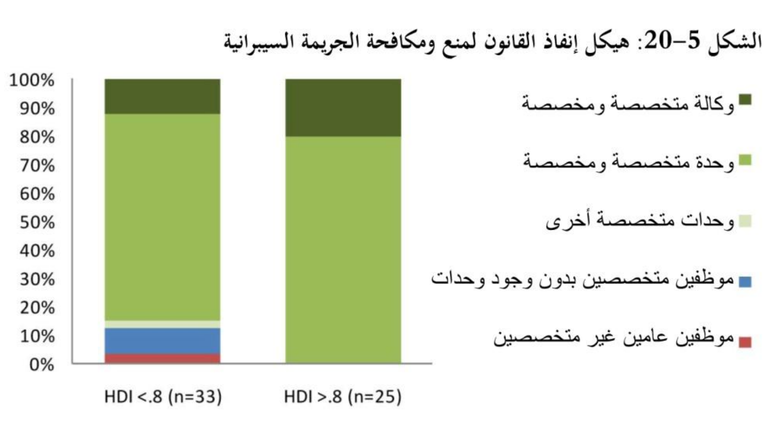
الموصولية بالإنترنت – أن يضطلع بشكل متزايد كافة الموظفين المكلفين بإنفاذ القانون بجمع الأدلة الإلكترونية، إلى جانب التعامل بشكل روتيني.

التخصص التنظيمي

أفادت أغلبية الدول المجيبة على الاستبيان الملحق بهذه الدراسة بوجود هياكل من سلطات إنفاذ القانون متخصصة في الجريمة السيبرانية، حيث أفاد ما يزيد عن نسبة 75 في المائة من الدول؛ بوجود وحدة متخصصة ومُكرّسة داخل الهيئات القائمة المنوط بها إنفاذ القانون. هذا وأفاد ما يقرب من نسبة 15 في المائة من الدول بوجود وكالة متخصصة ومُكرّسة للحالات المتعلقة إما بالجريمة السيبرانية أو المجال السيبراني.[1]

وجدير بالذكر، أن كلا من الدول الأكثر تقدما (HDI>0.8) والدول الأقل تقدما (HDI<0.8) قد أفادت بأهمية مستويات التخصص. وبالرغم من ذلك؛ قد أظهرت الدول الأقل نموا مجموعة عريضة من الهياكل، بيد أن بعض الدول أفادت بعدم وجود موظفين متخصصين، في حين ذكرت بعض الدول الأخرى وجود موظفين متخصصين ولكن غير مُعَدّين في وحدات مخصصة. ومع وجود استثناء وحيد (في أفريقيا)، أن الدول التي أفادت بافتقارها للوحدات أو الوكالات المتخصصة، أشارت إلى خطط لإنشاء واحدة في المستقبل القريب.[2]

الشكل 5–20: هيكل إنفاذ القانون لمنع ومكافحة الجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 113. (رقم=58)

أظهرت أيضا الدول المجيبة اختلافات عبر مستويات التنمية المتعلقة بطريقة إدماج الوحدات المتخصصة داخل إدارات وهيئات إنفاذ القانون على المستوى الفيدرالي أو الإقليمي أو على مستوى الدولة، أو على مستوى الشؤون المحلية. ففي بعض الدول؛ "لدى كافة هيئات التحقيق الفيدرالية وحدات مخصصة للجريمة السيبرانية".[3] وفي هذا السياق أيضا؛ أفادت دول أخرى أن الوحدات على المستوى الفيدرالي متغيرة مع ترتيبات إنفاذ القانون على مستوى الدولة والإقليم، وبين الولايات القضائية المختلفة.[4] ومن الملاحظ أن هناك أيضا تباينا كبيرا داخل الدول–حسبما

---

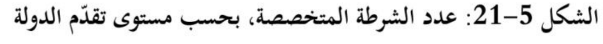
[1] الاستبيان الخاص بالدراسة، السؤال رقم 113
[2] المرجع السابق
[3] الاستبيان الخاص بالدراسة، السؤال رقم 113
[4] المرجع السابق

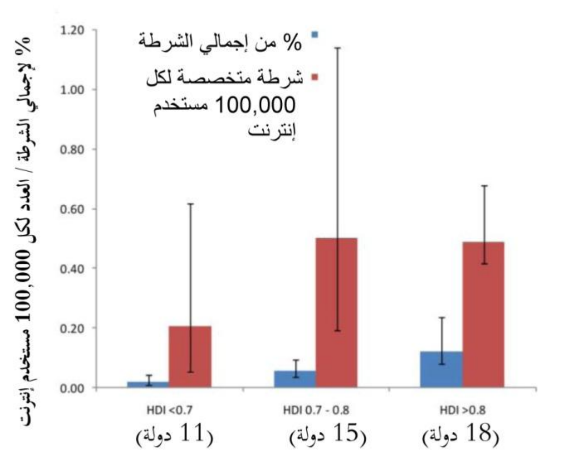
أفادت–من حيث التغطية الجغرافية وتَوَافُق الوحدات داخل هيئات أو وكالات إنفاذ القانون.[1] إلى جانب ذلك، فالعديد من الدول أفادت بإنشاء وحدة أو هيئة وطنية متخصصة مع وجود خطط تكميلية لإضافة موظفين ووحدات بشكل تزايدي في مواقع المكاتب الميدانية.

لطالَمَا أفادت الدول المتقدمة بوجود "مجموعة عريضة من المواد" أو "بكفاية الموارد"، بالرغم من أن العديد من هذه الدول أشارت إلى أن "الموارد تعتبر بشكل أساسي كافية لإجراء التحقيقات بهدف رفع مستوى القدرات إلى مستوى أعلى" و"تعتبر كل الموارد كافية لدرجة أنها تساعدنا على إنجاز هذه المهمة". ومن أجل تحسين النتائج وكفاءتها وسرعة إنجازها، فإننا نحتاج إلى موارد من الأجهزة والبرمجيات الجديدة والمتطورة.[2] أيضا، أشارت عدد من الدول الأكثر نموا إلى أن هناك متطلبات محددة تتمثل في تَنْمِيَة قدرات الموظفين، بما في ذلك، "عدم كفاية الموارد البشرية والاختلافات القائمة بين مستوى موارد أجهزة الشرطة على المستوى الفيدرالي ومستوى الولايات، إلى جانب أن مستويات الشرطة في بعض الولايات لديه من القدرات الكافية، بيد أن ذلك لا يتوفر لأجهزة الشرطة في بعض الولايات الأخرى.[3] كما أشارت الدول النامية في أفريقيا وآسيا إلى مُتَطَلّبَات تتعلق "بأدوات التحليل الجنائي عن بُعد"، حيث أكدت على أن "التحليل الجنائي الحاسوبي، وتطبيقاته" يعتبران من الأمور القديمة".[4]

الموظفون المتخصصون

أفاد العديد من الدول بوجود موظفين متخصصين مكلفين بإنفاذ القانون في الجريمة السيبرانية،[5] ولدى الدول الأقل نموا عدد أقل بكثير من أفراد الشرطة المتخصصين، بمعدل يبلغ نحو 0.2 لكل 100,000 مستخدم إنترنت ضمن البلد المعني، في حين يكون هذا المعدّل أعلى بمرتين إلى خمس مرات في البلدان التي تفوقها تقدما. أما نسبة الشرطة المتخصصة


الشكل 5–21: عدد الشرطة المتخصصة، بحسب مستوى تقدّم الدولة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 115 و61. (رقم=44)

---

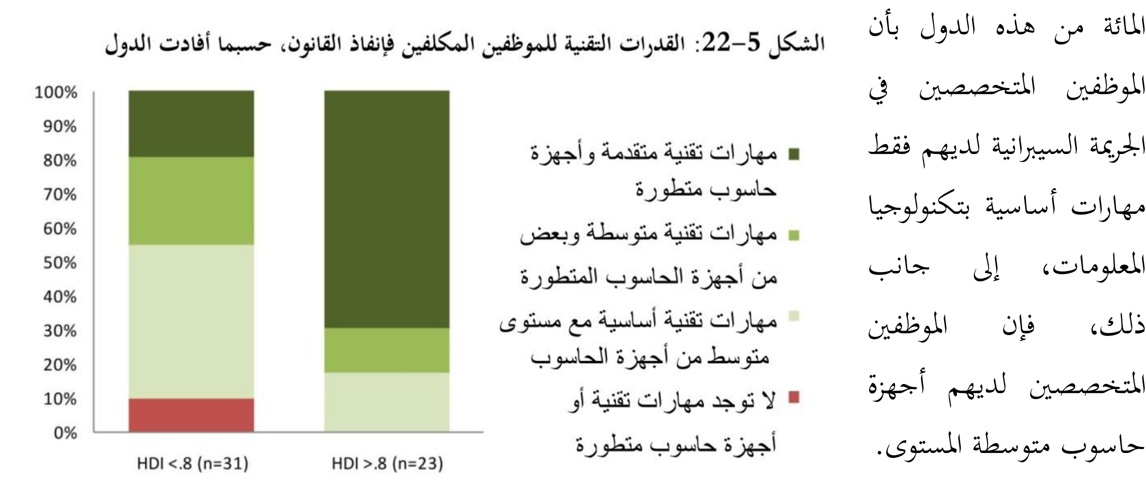
[1] المرجع السابق
[2] الاستبيان الخاص بالدراسة، السؤال رقم 109
[3] المرجع السابق
[4] المرجع السابق
[5] الاستبيان الخاص بالدراسة، السؤال رقم 115.

في الجريمة السيبرانية في كل الدول تمثلت في أقل من واحد في المائة من إجمالي الشرطة.[1]

وبإيجاز، فإن ما يقرب من نسبة 40 في المائة من الدول المجيبة؛ أفادت بأن الموظفين المتخصصين في الجريمة السيبرانية لديهم مهارات "متقدمة "خاصة بتكنولوجيا المعلومات، في حين أفاد ما يزيد عن نسبة 30 في المائة من الدول المجيبة بأن لديها موظفين متخصصين ولكن ذو مهارات "متوسطة". بيد أن نسبة 20 في المائة من الدول أشارت إلى أن الموظفين المتخصصين لديهم مهارات "أساسية" بتكنولوجيا المعلومات، إلى جانب ذلك، أفادت نسبة 6 في المائة من هذه الدول أن الموظفين المتخصصين ليس لديهم أي مهارات خاصة بتكنولوجيا المعلومات.

ومع ذلك؛ فإن هذه الصورة العامة تخفي اختلافات أساسية طبقا لمستوى نمو الدولة. ففي الدول الأعلى تقدما، قد أفادت نسبة 70 في المائة من الموظفين المتخصصين بامتلاك مهارات تقنية متقدمة، علاوة على أن لديهم أجهزة حاسوب مُتَطَوّرة. وعلى النقيض من ذلك؛ فإن في الدول الأقل نموا؛ ذكر ما يقرب من نسبة 45 في المائة من هذه الدول بأن الموظفين المتخصصين في الجريمة السيبرانية لديهم فقط مهارات أساسية بتكنولوجيا المعلومات، إلى جانب ذلك، فإن الموظفين المتخصصين لديهم أجهزة حاسوب متوسطة المستوى.

الشكل 5–22: القدرات التقنية للموظفين المكلفين فإنفاذ القانون، حسبما أفادت الدول



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 116. (رقم=54)

ومع ذلك، فإن الصورة داخل واحدة من هذه الدول قد تبدو مختلفة بشكل ملحوظ؛ فعلى سبيل المثال: أفادت إحدى الدول بأنه "لا يوجد تَقْرير عام مُتَيَسّر قدم نطاقا كاملا بشأن الوحدات المتخصصة"،[2] فبعض الوحدات لديها أجهزة وبرمجيات مناسبة، إلا أن مستوى مهارة (الموظفين) يعتبر غير كاف للتصدي للكثير من القضايا، في حين أن الوحدات الأخرى "مجهزة بموظفين متخصصين، ولكنها تفتقر إلى موارد متطورة".[3]

---

[1] تعتبر هذه الحسابات تأسيسا على الردود على السؤال رقم 115 الوارد في الاستبيان الخاص بالدراسة، بالإضافة إلى للدراسة الاستقصائية للأمم المتحدة بشأن لاتجاهات الجريمة وعمليات نظم العدالة الجنائية، (متاح آخر السنة).

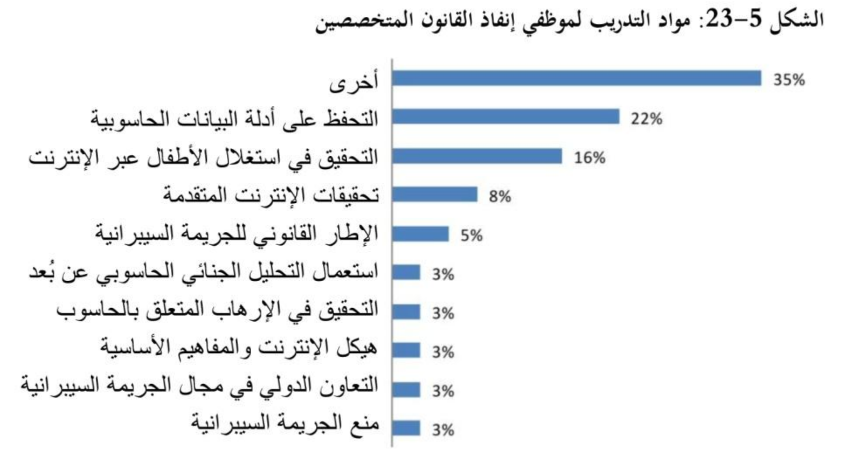
[2] الاستبيان الخاص بالدراسة، السؤال رقم 116

[3] المرجع السابق.

تنمية قدرات الموظفين

أفادت أغلبية الدول بأنها تقدم بعضا من التدريبات المتعلقة بالمجال السيبراني لكل من الموظفين المتخصصين والمكلفين بإنفاذ القانون والموظفين غير المتخصصين، حيث تلقى الموظفون المتخصصون والمكلفون بإنفاذ القانون تدريبا تناول مجموعة من الموضوعات بداية من التوجيه التقني وأسس التحقيقات إلى المسائل المتعلقة بجمع الأدلة الإلكترونية واستخدام أدوات التحليل الجنائي عن بُعد. هذا، وتناولت موضوعات التدريب متعددة المسائل المتعلقة (35 في المائة) بالتحفظ على الأدلة الحاسوبية (ما يقرب من 20 في المائة)، واستغلال الأطفال عبر الإنترنت (ما يقرب من 15 في المائة)، حيث يعتبر ذلك من المواد التدريبية الأكثر شيوعا لتدريب الموظفين المتخصصين. بالإضافة إلى ذلك؛ فهناك موضوعات أخرى تتعلق بالتدريبات، منها: التحقيقات المتقدمة بشأن الإنترنت، والتحليل الجنائي الرقمي، واستعمال برمجيات خاصة بالتحليل الجنائي، وتحليل البرمجيات الخبيثة.

الشكل 5–23: مواد التدريب لموظفي إنفاذ القانون المتخصصين



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 117. (رقم=37)

فمن الملاحظ التباين بشكل واسع في نطاق وتناول البرامج التدريبية التي حصل عليها الموظفون المتخصصون. ففي بعض الدول؛ فإن كافة الموظفين المتخصصين حصلوا على تدريبات متخصصة في الجريمة السيبرانية، إما عن طريق الحضور الشخصي أو عبر الإنترنت. بيد أنه في دول أخرى؛ يُمنح التدريب على المستوى الوطني للموظفين في وحدات مختارة بشأن المصطلحات الأساسية للجريمة السيبرانية أو المنهجية الأساسية للتحقيق. وفي هذا الصدد أيضا؛ أفادت بعض الدول بأنها تقدم برامج تدريبية إضافية تتعلق بموضوعات مثل الوعي الأساسي بتكنولوجيا المعلومات، والوعي بمواجهة الجرائم التقنية، والتحفظ على البيانات باعتبارها أحد الأدلة الإلكترونية، واستعمال أساليب التحليل الجنائي الحاسوبي عن بُعد. فالتدريب، حسبما أفادت الدول، إما يدخل في نطاق تدريب الموظفين المتخصصين أو يكون متاحا بقدر الحاجة إليه أو عند الطلب من قِبَل الموظفين.

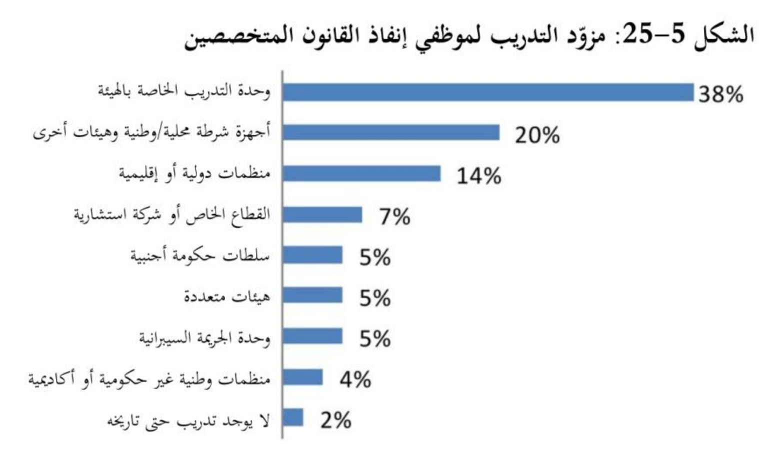
ويعتبر التدريب المنتظم أحد الأمور الهامة لتنمية قدرات الموظفين المكلفين بإنفاذ القانون، حيث تمكن الموظفين المتخصصين من إحاطتهم بأحدث التقنيات والتطورات. هذا وتتراوح نسبة التدريب المنتظم (أكثر من مرة واحدة في السنة) سواء في الدول الأكثر تقدما أو في الدول الأقل نموا – حسبما أفادت الدول – ما بين 50 في المائة إلى 60 في المائة. بيد أن بعض الدول الأقل نموا أفادت أنها، مع ذلك، تفتقر إما للتدريب أو لا يوجد تدريب متاح على الإطلاق.[1]

الشكل 5–24: تواتر التدريب لموظفي إنفاذ القانون المتخصصين

المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 118. (رقم=56)

وجدير بالذكر، أن المواد التدريبية للموظفين المتخصصين غالبا ما يحصلون عليها بشكل مباشر من قِبَل إحدى الوحدات التدريبية لهيئات إنفاذ القانون ذاتها. وذكرت المنظمات الإقليمية أو الدولية أنها تضطلع بتقديم مواد تدريبية للموظفين المكلفين بإنفاذ القانون والمتخصصين في الجريمة السيبرانية في ما يقرب من نسبة 15 في المائة من الدول، مما يدل ذلك على أحد الأدوار الهامة للمساعدة التقنية التي تتلقها الدول من قِبَل هذه المنظمات. ويتناول الفصل السادس (الأدلة الإلكترونية والعدالة الجنائية) بمزيد من التفصيل المتَطَلّبَات المعنية بالمساعدة الفنية، وتنفيذها.

الشكل 5–25: مزوّد التدريب لموظفي إنفاذ القانون المتخصصين

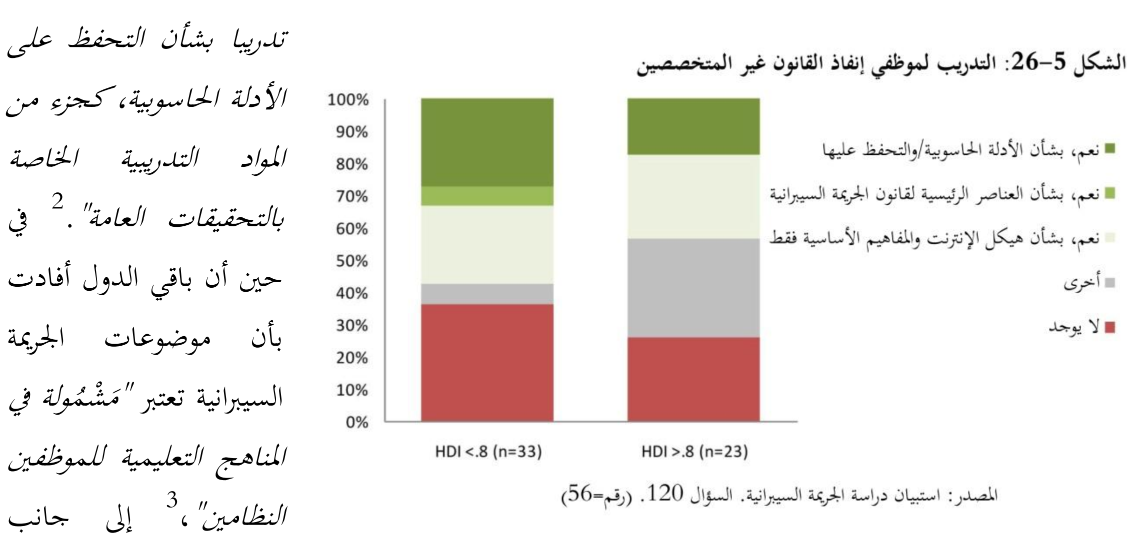


المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 119. (رقم=56)

[1] الاستبيان الخاص بالدراسة، السؤال رقم 118.

وباعتبار أن الأدلة الإلكترونية أصبحت إحدى عناصر التحقيق الهامة في كافة أنواع الجرائم، فإن المطلوب من موظفي إنفاذ القانون "غير المتخصصين" – بشكل متزايد – إجراء التحقيقات الأساسية المعنية بالأفعال ذات الصلة بالحاسوب. وفي هذا الصدد؛ أظهرت الردود على الاستبيان الخاص بهذه الدراسة اختلافات واضحة بين الدول فيما يتعلق بتنفيذ التدريبات المتعلقة بالجريمة السيبرانية للموظفين غير المتخصصين والمكلفين بإنفاذ القانون. هذا، وأفاد ما يقرب من نسبة 25 في المائة من الدول، سواء الأكثر تقدما أو الأقل نموا، بتلقي الموظفين غير المتخصصين تدريبا على هيكل الإنترنت والمفاهيم ذات الصلة به. ومع ذلك، فإن ما يقرب من نسبة 40 في المائة من الدول الأقل نموا أفادت بأن الموظفين غير المتخصصين لا يحصلون على أي تدريب بشأن الجريمة السيبرانية أو الأدلة الإلكترونية. وبالرغم من ذلك؛ أبدى عدد من الدول مبادرات لتحسين التدريب المتعلق بالجريمة السيبرانية للموظفين غير المتخصصين. وفي هذا السياق، أفادت إحدى الدول، على سبيل المثال، "اتَّخَذَت مُبَادَرَة بشأن "توحيد" البرامج التي تدرس لكل الموظفين، وذلك لمنحهم مفهوم أساسي بماهية الجريمة السيبرانية والتقنيات ذات الصلة بالتحقيقات والتشريعات".[1] بيد أن إحدى الدول الأخرى أشارت إلى أن *"الموظفين النظامين يتلقون تدريبا بشأن التحفظ على الأدلة الحاسوبية، كجزء من المواد التدريبية الخاصة بالتحقيقات العامة"*.[2] في حين أن باقي الدول أفادت بأن موضوعات الجريمة السيبرانية تعتبر *"مَشْمُولة في المناهج التعليمية للموظفين النظامين"*،[3] إلى جانب *"إتاحة التدريب، للموظفين الراغبين في ذلك، من خلال دورات تدريبية عبر الإنترنت في برامجنا المعنية بالتدريب التقني"*.[4]

الشكل 5–26: التدريب لموظفي إنفاذ القانون غير المتخصصين



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 120. (رقم=56)

[1] الاستبيان الخاص بالدراسة، السؤال رقم 120.
[2] المرجع السابق
[3] المرجع السابق
[4] المرجع السابق

الفصل السادس: الأدلة الإلكترونية والعدالة الجنائية

يتناول هذا الفصل عملية العدالة الجنائية في حالات الجريمة السيبرانية، بدءا من الحاجة إلى تحديد وجمع وتحليل الأدلة الإلكترونية من خلال الأدلة العدلية الرقمية. ويستعرض مقبولية واستخدام الأدلة الإلكترونية في المحاكمات الجنائية، فضلا عن أنه يعرض كيف يمكن لمجموعة من التحديات القضائية أن تؤثر على أداء نظام العدالة الجنائية. ويربط الفصل بين إنفاذ القانون واحتياجات قدرة العدالة الجنائية الهادفة إلى أنشطة المساعدة الفنية، المقدمة واللازمة.

1-6 مدخل إلى الأدلة الإلكترونية والأدلة العدلية الرقمية

الاستنتاجات الرئيسية

- الأدلة هي الوسائل التي تربط الوقائع بإدانة وإبراء الأفراد أثناء إقامة المحاكمات. الأدلة الإلكترونية هي جميع المواد الموجودة في شكل إلكتروني أو رقمي
- تهتم الأدلة العدلية الرقمية باستعادة – عادة ما تكون متقلبة وسهلة الإفساد – المعلومات التي قد يكون لها قيمة دلالية
- تتضمن تقنيات الأدلة الجنائية إيجاد نسخ "شيئا فشيئا" من المعلومات المخزنة أو المحذوفة، "منع الكتابة" من أجل ضمان أن المعلومات الأصلية لم يتم تغييرها، وأن ملفات التشفير "أدوات التشفير"، أو التوقيعات الرقمية، التي يمكن أن تبين التغييرات في المعلومات

الأدلة الإلكترونية في الإجراءات الجنائية

الأدلة هي الوسائل التي تربط الوقائع بإدانة وإبراء الأفراد أثناء إقامة المحاكمات. الأدلة الإلكترونية هي جميع المواد الموجودة في شكل إلكتروني أو رقمي، وكما هو ملاحظ في الفصل الأول (التواصل العالمي)، فإن الأدلة الإلكترونية هي أمر محوري ليس فقط فيما يخص التحقيق والقضاء لأشكال الجريمة السيبرانية، ولكن تتزايد فيما يخص الجريمة على نحو عام. تعد الإطارات القانونية المثلى للأدلة جنبا إلى جنب مع إنفاذ القانون وقدرة العدالة الجنائية على تحديد وجمع وتحليل الأدلة الإلكترونية، أمرا جوهريا للحصول على استجابة فعالة للجريمة.

وأثناء مرحلة جمع المعلومات لدراستها، تم طرح أسئلة على البلدان حول قدرة سلطات إنفاذ القانون والمدعين العامين على جمع وتناول الأدلة الإلكترونية، كما تم طرح أسئلة على البلدان حول الإطارات القانونية

للأدلة الإلكترونية، بما في ذلك مقبولية واستدلالية القوانين والقواعد التي تطبق على الأدلة الإلكترونية[1]. وقبل النظر في استجابات البلدان، فيتضمن هذا القسم مقدمة موجزة إلى طبيعة الأدلة الإلكترونية والوسائل التي يمكن جمعها من خلالها، بما في ذلك الأدلة العدلية الرقمية.

جمع الأدلة – ينتج عن تفاعل المستخدم مع أجهزة الحاسوب مجموعة كبيرة من الآثار الرقمية (يطلق عليها أحيانا البصمات الرقمية أو الأشياء الاصطناعية). وقد تحتوي بيانات الحاسوب والاتصالات الإلكترونية التي يحتمل أن تكون ذات صلة بعمل إجرامي على العديد من غيغابايت من الصور والفيديوهات ورسائل البريد الإلكتروني وسجلات المحادثات وبيانات النظام. ويمكن أن يكون تحديد المعلومات ذات الصلة داخل هذه البيانات مستنفذا للوقت. وكذلك يصب تنوع أشكال الملفات المحتملة ونظام التشغيل والبرمجيات التطبيقية وتفاصيل الأجهزة في تعقيدات عملية تحديد المعلومات ذات الصلة.

يمكن تعديل الأشياء الاصطناعية الخاصة بالحاسوب أو الكتابة فوقها أو حذفها بسهولة، الأمر الذي يطرح تحديات حيث يجب المصادقة والتحقق من مصادر المعلومات الرقمية.[2] وتختلف قواعد الأدلة اختلافا ملحوظا بين الولايات القضائية، حتى بين البلدان ذات أعراف قانونية متشابهة. وبصورة عامة، ومع ذلك فإن الأنظمة القانونية لأعراف القانون العام تميل إلى أن تحظى بقواعد محددة فيما يخص مقبولية الأدلة. وفيما يخص الأنظمة القانونية لأعراف القانون المدني التي يحتفظ فيها القضاة المختصون بدرجة عالية من السيطرة على إجراءات المحكمة، فقد تكون مقبولية الأدلة مرنة على الرغم من أن ترجيح الأدلة (بما في ذلك التأكد من مصداقيتها وصحتها) يمكن أن يمتثل أيضا لمجموعة شاملة من القواعد.[3]

وفي العديد من الأنظمة القانونية، يجب على مؤيدي الأدلة عرض جودة الإجراءات المطبقة للحفاظ على سلامة المعلومات الرقمية بدءا من لحظة إنشائها ووصولا لمرحلة تقديمها أمام المحكمة. لسلامة وصحة المعلومات الرقمية تأثير مباشر على ترجيح الأدلة من حيث الموثوقية والجدارة بالثقة. فيجب على الطرف الذي يسعى إلى تقديم أدلة أن يعرض استمرارية الأدلة دائما، أو "سلسلة المسؤوليات" بحيث يمكن إثبات أنه لم يتم العبث بالأدلة أو تغييرها بخلاف ذلك. تعد استمرارية الأدلة بمثابة مسألة واقعية، فضلا عن أن عملية سلسلة المسؤوليات هي الآلية المطبقة فيما يخص حفظ وتوثيق التاريخ الزمني للأدلة حيث أنه يتحرك من مكان إلى آخر.[4]

وفي حالة المعلومات الرقمية، فيجب الحفظ على استمرارية الأدلة على كل من الأجهزة المادية التي تحتوي على البيانات (عند تلقيها أو الاستيلاء عليها)، والبيانات المخزنة الموجودة على الأجهزة.[5] وعلى هذا النحو،

---

[1] أنظر دراسة استبيان الجرائم السبرانية Q109-112، و Q143-150.

[2] أنظر على سبيل المثال *قضية الولايات المتحدة ضد ويتاكر*، (7th Cir. 1997) 127 F3d 595, 602.

[3] أنظر جاكسون، جيه دي، وسامرز، اس. جيه، 2012. *تدويل الأدلة الجنائية: ما وراء أعراف القانون العام والقانون المدني*. كامبريدج: مطبعة جامعة كامبريدج.

[4] كيسي، إي.، 2011. *الأدلة الرقمية وجرائم الحاسوب: علم الأدلة الجنائية، أجهزة الحاسوب والإنترنت*. نيويورك: إلسفير.

[5] وزارة العدل الأمريكية، 2007. *الأدلة الرقمية الموجودة في حجرة المحكمة: دليل لإنفاذ القانون والمدعيين العامين. معهد العدالة الوطني*، صفحة: 16.

يجب على الطرف الذي يقدم الأدلة عرض التالي: (1) أن المعلومات الرقمية التي تم الحصول عليها من الجهاز هي بمثابة تمثيل حقيقي وسليم للبيانات الأصلية التي يتضمنها الجهاز (الصحة) ؛ (2) وأن الجهاز والبيانات المراد تقديمها بصفتها أدلة هي ذاتها التي تم اكتشافها في الأصل وتم إدراجها سلسلة المسؤوليات (السلامة). ويكمن الهدف في إظهار أن الجهاز هو ما يفترض أن يكون، وأن المعلومات الرقمية جديرة بالثقة ولم يتم العبث فيها أو تغييرها.[1]

تم الطعن أيضا في موثوقية المعلومات المولدة من الحاسوب وتلك المخزنة على الحاسوب على أساس الثغرات الأمنية الموجودة في أنظمة التشغيل والبرامج التي يمكن أن تؤدي إلى طرح تهديدات على سلامة المعلومات الرقمية. وقد نظرت المحاكم في قابلية المعلومات الرقمية للتعرض للتلاعب أثناء تقديم الدلائل الإلكترونية، فضلا عن تسليط الضوء على '*الحاجة لتبيان صحة الحاسوب فيما يخص قدرته على الاحتفاظ بالمعلومات موضوع القضية واستعادتها*"[2] إن مقبولية المعلومات المتولدة من الحاسوب (مثل سجلات ملف التسجيل) تعطي تفاصيل عن الأنشطة الخاصة بالحاسوب، والشبكة وغيرها من الأجهزة التي يمكن أن تكون عرضة للطعن في حال كان النظام الذي يقوم بتوليد المعلومات لا يحتوي على ضوابط أمنية قوية.[3]

وبالإضافة إلى عرض صحة وسلامة الأدلة، تنشأ الطعون في استخدام الأدلة الإلكترونية، في بعض الولايات القضائية، نتيجة تطبيق قواعد دلالية معينة. وربما تكون في حاجة إلى أن يتم عرضها، وعلى سبيل المثال، تلك الأدلة الإلكترونية التي تقع ضمن استثناءات معينة لفرض حظر عام على "الإشاعات" الأدلة،[4] أو تلك "المطبوعة" من بيانات الحاسوب والتي تلبي المتطلبات مثل قاعدة "الدليل الأفضل".[5] يتناول هذا الفصل المناهج الوطنية لمثل هذه القضايا المنوه عنها في استبيان الدراسة.

---

[1] مارسيلا الابن، آيه جيه، غرينفيلد،أر. اس، (محرران)، 2002. الأدلة الجنائية الإلكترونية: *الدليل الميداني لجمع ودراسة وحفظ أدلة جرائم الحاسوب*، النسخة الثانية. بوكا راتون: مطبعة سي أر سي، الصفحة: 136.

[2] *ري فيبي فينهي، قضية شركة ديبتور أمريكان إكسبريس ترافل ريلاتد سيرفيس، ضد شركة فيبي فينهي*9th Cir BAP) 437 BR 336 16 ديسمبر، 2006) صفحة: 18.

[3] تشايكين، دي. 2006. تحقيقات الشبكة حول الهجمات الإلكترونية: حدود الأدلة الرقمية. *الجريمة والقانون والتغير الاجتماعي*، 46 (4 -5): 239 – 265، 249.

[4] عادة ما يتم تعريف الإشاعة على أنها " الأدلة المقدمة عن بيان أدلى به في بعض المناسبات الأخرى، عندما يقصد بها أن تكون بمثابة دليل على حقيقة ما جرى التأكيد عليه' (قوانين هالبري، المجلد 17). قد تشكل بدقة أنواع معينة من الأدلة الرقمية الإشاعات، ولكن يمكن قبولها تحت استثناءات مثل "السجلات التجارية". أنظر طومسون، 2011LL. مقبولية الوثائق الإلكترونية بصفتها أدلة في المحاكم الأميركية. الملحق 9، ب. 1، مركز للمكتبات البحثية ودراسة الأدلة الالكترونية لحقوق الإنسان".

[5] بصفته مبدأ عام، يحق للمحاكم الحصول على أفضل الأدلة المتاحة. وفي حالة تطبيق قاعدة أفضل الأدلة، فقد تنتفي مقبولية النسخ الأصلية بصفتها أدلة ما لم كان يمكن عرض أن الأصول غير متوفرة نظرا لتلفها أو لظروف أخرى. وقد لا يتم اعتبار المعلومات المطبوعة من أي حاسوب أو غيره من أجهزة التخزين بمثابة "أصول". وفي بعض الولايات القضائية، على الرغم من أن قاعدة الأدلة الأفضل لا تقتضي استبعاد المطبوعات، شريطة أن تعكس المطبوعات البيانات الفعلية بدقة. أنظر على سبيل المثال، قضية دو ضد الولايات المتحدة، 805 ملف. ملحق. 1513، 1517 (دي. هاواي 1992)؛ ولوغنر ضد الولاية، 769 N.E.2d 1147, 159 (إنديانا. Ct. التطبيق. 2002).

الأدلة الجنائية الرقمية

قد تكون العديد من أشكال الأدلة الإلكترونية صريحة نسبيا، مثل مطبوعات رسائل البريد الإلكتروني المتوفرة بسهولة التي يرسلها مرتكب الجريمة، أو سجلات اتصال بروتوكول الإنترنت التي يبلغ عنها مباشرة من قبل موفر خدمة الإنترنت. ومن جانب آخر، قد تتطلب أشكال أخرى تقنيات متطورة من أجل استعادة آثار الأنشطة أو البيانات التي يتم الحصول عليها من الحاسوب والشبكات التي من شأنها أن تقدم أدلة على سلوك إجرامي. تشكل الأدلة العدلية الرقمية فرعا من العلوم الجنائية المعنية باستعادة وإجراء تحقيق بشأن المواد التي تم الحصول عليها من الأنظمة الرقمية وأنظمة الحاسوب. ولتعقب هذه الآثار، يستفيد خبراء الأدلة العدلية الرقمية من قابلية الحواسيب لتخزين وتسجيل وحفظ بيانات عن أغلب الأنشطة التي تقوم بها، وبالتالي التي يقوم بها مستخدموها.

سيناريو الأدلة الجنائية: أدلة التحايل عبر الحاسوب من أحد مقاهي الإنترنت

سيناريو: تم القيام بمحاولة احتيال عبر البريد الإلكتروني. حصلت الشرطة على أدلة تفيد بأن أن رسائل البريد الإلكتروني المعنية قد تم إرسالها من حاسوب مكتبي في مقهى إنترنت محلي

إعداد نموذجي لمقهى إنترنت يشبه بيئة الشبكة المنزلية في العديد من النواحي. ومن المحتمل أن تتضمن العديد من أجهزة الحاسوب المحمول أو الحاسوب المكتبي المتصلة عبر مزيج من أجهزة الشبكات المتصلة اللاسلكية والسلكية. وفيما يخص أغراض فواتير أجهزة الحاسوب ومقاهي الإنترنت، فقد تتطلب التحقق من هوية المستخدم؛ ويكون هذا إلزاميا في العديد من الولايات القضائية، فضلا عن أنه يوفر خط سير مراجعة لربط الأفراد بأي أجهزة حاسوب معنية في أي وقت معين. وقد يكون من الممكن أيضا تحديد أي فرد يستخدم أي حاسوب في أي وقت من خلال لقطات تلتقطها كاميرات المراقبة.

في حالة إجراء تحقيق سريع بما فيه الكفاية، أو في حال وجود علم مسبق بالأنشطة، فمن ثم قد يكون محققوا الأدلة الجنائية في وضع يمكنهم من الوصول الفعلي إلى الحاسوب وإجراء تحقيق معياري. وتزداد تعقيدات هذه العملية نتيجة للطابع العام للجهاز، والذي يحتوي بدوره آثارا لنشاط الكثير من المستخدمين.

وعادة ما تتعامل مقاهي الإنترنت مع الكثير من المستخدمين وحركة بيانات مقارنة بالشبكة المنزلية، ويرجح أن تحظى بأجهزة شبكة إضافية مثل خوادم بروكسي التي تحتفظ بنسخ من صفحات الويب المطلوبة عادة من أجل تسريع حركة الاتصالات؛ وأجهزة جدار الحماية الخاص بالتأمين. ويمكن تحليل هذه الأجهزة فيما يخص آثار نشاط الشبكة المرتبطة بالأنشطة المشبوهة للمستخدم.

إن المعلومات المخزنة على الأجهزة الإلكترونية، بما في ذلك أجهزة الحاسوب والهواتف المحمولة هي معلومات متقلبة ويسهل تغييرها أو العبث بها أثناء التحقيقات. وفي الوقت ذاته، فإن هذه المعلومات من السهل مضاعفتها. ولذلك فإن إحدى الخطوات الأولية الهامة في العديد من التحقيقات القائمة على الأدلة العدلية الرقمية هي إيجاد صورة أدلة جنائية غير مضطربة (أو نسخ مطابقة تماما) لجهاز التخزين، تحتوي على نسخة من الجهاز الأصلي مفصلة بقدر الإمكان. ومن خلال العمل على الصورة بدلا من الجهاز الأصلي، فيمكن فحص البيانات دون إلحاق أي

اضطراب بالنسخة الأصلية، لذا نوفر حماية ضد أي تلاعب أو تزوير. وعادة ما يتم إيجاد صورة الأدلة الجنائية بمساعدة جهاز مختص يطلق عليه مانع الكتابة والذي من شأنه منع إلحاق أي تغييرات على البيانات الأصلية.[1]

وبالإضافة إلى القدرة على إيجاد نسخة "خطوة بخطوة" للمعلومات المخزنة، وغيرها من أدوات الأدلة الجنائية الهامة بما في ذلك استخدام برامج "نحت البيانات" أو "نحت الملفات" والتي من شأنها استعادة الملفات المحذوفة أو التالفة من بقايا البيانات الأولية التي تبقى على أجهزة التخزين حتى بعد زوال الملف الأصلي.[2] بالإضافة إلى أنه لمقارنة الملفات بسرعة وبدقة، تستخدم أدوات التحليل تجزئات التشفير التي تتوافق مع 'توقيع' صغير وفريد من نوعه لجزء معين من البيانات. إذ أن أي تغيير بسيط للبيانات ينتج عنه حدوث تشفير مختلف.

تتطلب أجهزة مختلفة نوعية مختلفة من تقنيات التحقيق والأدلة الجنائية. ويتطلب فحص أجهزة المحمول مجموعة مختلفة من الأدوات مقارنة بتلك التي يتم استخدامها عند فحص جهاز حاسوب مكتبي أو خادم شبكة. تعرض الأنواع المختلفة من

سيناريو الأدلة الجنائية: أدلة تم الحصول عليها من حامل متنقل بخصوص مؤامرة لارتكاب جريمة خطيرة

سيناريو: التحقيق مع أحد الأفراد قيد الاتهام بالتآمر لارتكاب جريمة قتل. وكجزء من هذا التحقيق، طلبت الشرطة الحصول على بيانات من شبكة الهاتف المحمول الذي يستخدمها هذا الفرد.

تتشابه قدرات مقدمي خدمات الهاتف المحمول مع مقدمي خدمات الإنترنت، بجانب إضافة هامة ألا وهي البيانات الخاصة بتحديد الموقع الجغرافي والتي تكشف عن الموقع المادي لأي مستخدم.

ستقوم بيانات حركة اتصالات الهاتف، في أغلب الولايات القضائية، بتخزين أرقام الهواتف التي تم الاتصال بها فضلا عن زمن الاتصال ومدته. تعمل قدرات التنصت بنفس القدر التي يعمل به مقدمو خدمات الاتصالات الهاتفية الأخرى. ويمكن أن تكشف هذه المعلومات عن أنماط الاتصالات الصادرة إلى أفراد آخرين، فضلا عن توفير ارتباطات بين الأحداث التي وقعت في العالم الحقيقي، مثل إجراء مكالمة هاتفية قصيرة قبل ارتكاب جريمة ما.

ومع ذلك يكمن الاختلاف الأكبر ملاحظة بين الهواتف المحمولة في أنه عادة ما يقوم المالك بحمل الجهاز في جميع الأوقات، ويتصل باستمرار بمحطات أساس المحمول المحلية التي تنقل إشارات الهاتف. ومن خلال تعقب محطات الأساس التي يتصل بها الهاتف في أي وقت معين، فيمكن الاستدلال على موقع المالك داخل أي منطقة معينة. فإذا ما تم النجاح في عمل مثلث بالعديد من محطات الأساس بفعالية؛ فيمكن حصر مكان الهاتف داخل نطاق عشرات الأمتار.

وبالاعتماد على الولاية القضائية وسياسات الاحتفاظ بالبيانات، فربما يقوم مقدمو الخدمات بتخزين المواقع الجغرافية للهواتف المحمولة في أي وقت تتلقى فيها رسائل أو مكالمات هاتفية، كما هو الحال فيما يتعلق بتوصيات الاتحاد الأوروبي المتعلقة بالإبقاء على البيانات. وقد لا تقوم ولايات قضائية أخرى بتخزين هذه البيانات إطلاقا، ما عدا حينما تطلب جهات إنفاذ القانون هذا صراحة، وفي هذه الحالة يمكن السماح بإجراء تثليث الموقع بُغية تحديد موقع الأفراد بدقة من خلال هواتفهم.

[1] المعهد الأمريكي الوطني للمعايير والتكنولوجيا، 2004. *جهاز مانع الكتابة (HWB) مواصفات، الإصدار 2.0.*

[2] غوتمان، بي.، 1996. الحذف الآمن للبيانات من الذاكرة المغنطيسية وذاكرة الحالة الصلبة. *وقائع الندوة الأمنية السادسة لاتحاد الحوسبة التقنية المتقدمة.*

الأجهزة والبرمجيات وأنظمة التشغيل التحديات التي تمثلها فيما يتعلق باستعادة المعلومات.

تركز *الأدلة الجنائية الحاسوبية* على تحليل أجهزة الحاسوب المكتبي والحاسوب المحمول على النحو الموجود في المنازل وأماكن العمل. عادة ما تحتوي أجهزة الحاسوب على أقراص صلبة ذات سعة كبيرة من شأنها تخزين كمية كبيرة من المعلومات، بما في ذلك الصور ومقاطع الفيديو، فضلا عن تواريخ تصفح المواقع الإلكترونية ورسائل البريد الإلكتروني ومعلومات التراسل الفوري. وعادة ما تقوم بتشغيل عدد صغير من أنظمة التشغيل المشهورة بما في ذلك ويندوز، ماك أو إس، لينوكس.

تقوم الأدلة الجنائية القائمة على أجهزة المحمول بفحص أجهزة المحمول التي تعمل بطاقة منخفضة، ذات سعة تخزين أقل، مقارنة بأجهزة الحاسوب، وذات برامج أبسط لتسهيل المكالمات الهاتفية وتصفح الإنترنت. ومع ذلك فإن الفجوة الموجودة بين الهواتف وأجهزة الحاسوب هي التوجه إلى الصغر من حيث الوظائف والطاقة التشغيلية والبرمجيات. أن إحدى السمات المميزة لأجهزة المحمول هي قابليتها على التنقل – فهي عادة ما تكون بصحبة مالكها في كل الأوقات – واتصالها المستمر. وهذا ما يساعد على الحصول على مراقبة للموقع الجغرافي دقيقة إلى حد معقول في النظم الحديثة. عادة ما تحتوي على كل من قائمة جهات الاتصال كاملة نسبيا، فضلا عن سجلات المكالمات. كما تتدفق عادة جميع البيانات والمعلومات عبر شبكات مقدمي خدمات إنترنت المحمول، مما يمكِّن المحققين من

مثال حالة: تحديد ابتزاز على الإنترنت (بلد في أمريكا الشمالية)

تعرض إحدى تحقيقات إنفاذ القانون في عملية ابتزاز مزعومة بعض التقنيات المستخدمة في تعقب المجرمين عبر الإنترنت. في هذه الحالة هدد المتهم بنشر صور جنسية لضحاياه على صفحات شبكات التواصل الاجتماعي الخاصة.

تلقى المحققون معلومات من قسم الأمن الخاص بموقع شبكة التواصل الاجتماعي حول تسجيل الدخول إلى الحسابات الخاصة بالضحايا، فجميعهم يتأصلون من عنوان بروتوكول إنترنت واحد. قام أحد المتهمين بالوصول إلى 176 حساب مختلف من خلال عنوان بروتوكول إنترنت واحد في أقل من شهرين، وأغلبهم من على جهاز حاسوب واحد. ولقد قام العديد من مستخدمي هذه الحسابات بتعطيل حساباتهم عقب اختراقها. ولقد تم استخدام نفس عنوان بروتوكول الإنترنت للوصول إلى الحساب الخاص بالمتهم 190 مرة أكثر من أي عنوان آخر. ولقد تم استخدامه أيضا لتسجيل الدخول 52 مرة إلى حسابات البريد الإلكتروني الخاص بأحد الضحايا. وظهر تسجيل دخول منفصل إلى حساب المتهم من عنوان بروتوكول إنترنت مسجل باسم شركة مدرجة بصفتها صاحب عمل المتهم على صفحته الشخصية بشبكات التواصل الاجتماعي. ومن هذا المنطلق، فقد تم تقديم طلب إلى مقدمي خدمات الإنترنت للحصول على معلومات مشترك متصل بعنوان بروتوكول الإنترنت. وفي غضون أسبوع واحد، قام مقدمو خدمة الإنترنت المسؤولين عن عنوان بروتوكول الإنترنت الخاص بالمتهم بتقديم معلومات المشترك، بما في ذلك العنوان المادي الذي يطابق السجلات العامة الأخرى. قام المحققون بتحرير مذكرة تفتيش لهذا المبنى، والسيطرة على المزيد من الأدلة التي استخدمت لإدانة المتهم لاحقا في نفس الشهر.

المصدر: http://www.justice.gov/usao/cac/Pressroom/2013/016.html ، http://arstechnica.com

الحصول على مجموعة كبيرة من المعلومات المتعلقة باستخدام الهاتف. والأجهزة اللوحية غالبا ما تكون بمثابة نسخ مطورة من أجهزة المحمول الأمر الذي يجعل الأدوات المصممة لأجهزة المحمول مطبقة أيضا.

وتحظى تقنيات *الأدلة الجنائية الخاصة بالشبكة* بأهمية حاليا حيث ترتبط بالهواتف المحمولة وأجهزة الحاسوب فضلا عن العديد من الإجراءات التي تستخدم من أجلها خدمات الإنترنت والتخزين السحابي. وتخزن تلك الخدمات البيانات على الإنترنت بدلا من تخزينها على جهاز المستخدم، الأمر الذي يقلل من كمية المعلومات التي يمكن تجميعها بدون استخدام تحليل الشبكة. ويكون نقل بيانات الشبكة مؤقتا في العموم. وللحصول على معلومات مفصلة بخصوص الأنشطة التي تجري في الشبكة، يتعين جمع البيانات بصورة نشطة وتخزينها للتحليل لاحقا. ويمكن أن يشمل هذا تحليلا لملفات السجلات من أجهزة الشبكة مثل جدران الحماية وكشف التسلل فضلا عن نظم الوقاية وكذلك تحليل محتوى نقل بيانات الشبكة المسجلة في حال توفرها.[1]

وفي المواقف التي قد ينجح فيها المهاجم في الوصول الإلكتروني لأحد أنظمة الحاسوب، تصبح أي بيانات على هذا الحاسوب معرضة للخطر من طرف المهاجم. وفي هذه الحالات، قد لا يعتد بملفات السجلات لنشاط هذا النظام، ولا تمثل التحقيقات الجنائية للشبكة الصيغة الوحيدة المتاحة لأي محلل. ويكمن التحدي الأساسي في التحقيق الجنائي لأي شبكة في إعادة القيام بالإجراءات التي اتخذت على أي شبكة من بيانات السجلات المحدودة المتاحة. وقد يستخدم هذا بتحديد محاولات التسلل والوصول غير المصرح به للأنظمة ومحاولة قطع الخدمة، إضافة إلى البيانات بشأن أي الموارد التي وصل إليها الأفراد في أي وقت.

[1] Chappell, L., 2012. Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide. Laura Chappell University

2-6 القدرة على التعامل مع الأدلة الجنائية (العدلية) الرقمية والأدلة الإلكترونية

الاستنتاجات الرئيسية

- بينما تمتلك معظم البلدان بعض قدرات الأدلة العدلية، أفادت العديد من الدول المجيبة، في جميع المناطق، بوجود عدد غير كافٍ من المحققين الجنائيين، والاختلاف بين القدرات على المستوى الاتحادي والمحلي، ونقص أدوات التحقيق الجنائي، وتأخر الأعمال نتيجة للكميات الضخمة من البيانات التي تستلزم التحليل
- أبلغت أكثر من نصف الدول أن المشتبه فيهم يستخدمون التشفير، مما يؤدي إلى صعوبة الوصول إلى هذا النوع من الأدلة وضياع الوقت دون فك الشفرات
- وتفيد جميع الدول في أفريقيا وثلث دول المناطق الأخرى عدم كفاية الموارد للمدعين للتعامل مع هذه الأدلة الإلكترونية وتحليلها
- الأدلة الإلكترونية معترف بها في المحكمة بأكثر من 85 في المائة من البلدان المجيبة، وذلك مع قلة عدد العوائق القانونية مثل عدم الاعتراف بجميع الأدلة الإلكترونية وعدم الاعتراف بالأدلة الإلكترونية خارج حدود الدولة والعوائق الخطيرة الحالية التي تواجه مقاضاة أفعال الجريمة السيبرانية

قدرات الأدلة الجنائية

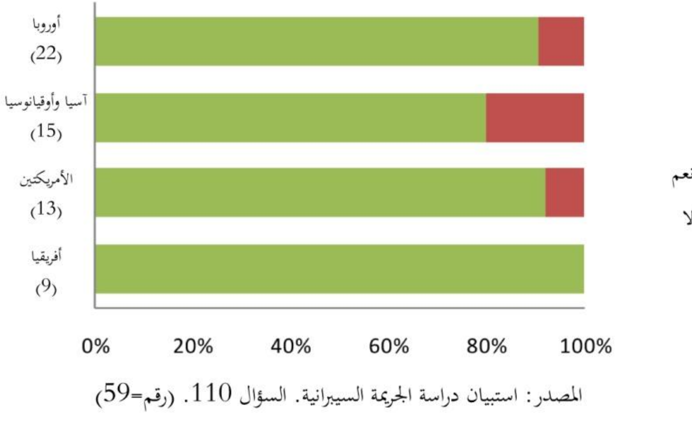
يمكن أن تكون قدرات جهات إنفاذ القانون على تجميع الأدلة الإلكترونية وتحليلها أثناء التحقيقات حاسمة في النجاح في التعرف على مرتكبي الانتهاكات ومقاضاتهم. وقد أوضحت البلدان المجيبة على الاستبيان الملحق بهذه الدراسة مجموعة من القدرات في هذا الشأن. وقد أفادت أكثر من 90 في المائة من البلدان، في جميع مناطق العالم، بعض القدرة على إجراء تحقيقات تعتمد على الأدلة الجنائية (العدلية) الرقمية.[1] وتشير المعلومات الإضافية المقدمة من البلدان بشأن الوصول إلى المصادر الجنائية ومستويات القدرة، برغم ذلك، إلى صورة متباينة. وقد أفاد أقل من نصف البلدان في أفريقيا وحوالي ثلثي بلدان الأمريكتين كفاية موارد إنفاذ القانون (مثل الكهرباء والأجهزة والبرامجيات والوصول إلى الإنترنت) من أجل إجراء التحقيقات وتحليل الأدلة الإلكترونية.[2] وفي المقابل، أفاد ما يصل على 80 في المائة من البلدان في أوروبا وآسيا وأوقيانوسيا كفاية الموارد.

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 110.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 109.

ولكن أفادت بلدان عدة مثل بعض الدول المتطورة وجود تحديات مرتبطة بمعالجة كميات كبيرة من البيانات وزيادة عدد الأدلة المقدمة من أجل التحليل الجنائي.[1] أفادت إحدى البلدان في أوروبا، على سبيل المثال: "*على المستوى القومي، الشرطة قادرة على إجراء مستوى عالٍ من التحقيق الجنائي الحاسوبي. وعلى مستوى المقاطعات والمستوى المحلي لا تتوفر إلا القدرة على إجراء العمل الجنائي الحاسوبي الأساسي*". وقد أفاد البلد ذاته: أن "زيادة عدد الأدلة الإلكترونية التي يجري الحصول عليها أثناء التحقيق في جميع أنواع الجرائم، تشكل تحديا لاسيما بالنسبة للشرطة المحلية التي تتعامل مع عدد كبير من الحالات". وعلى غرار ذلك، سلطت إحدى بلدان الأمريكتين الضوء على أن: "*التحدي لا يكمن في الخبرة، وإنما في كمية البيانات التي يجب تحليلها.*"[2] بينما أشار بلد آخر أن: "*كم المعلومات والبيانات التي يجري الحصول عليها ينتج عنه المزيد والمزيد من المشكلات بالنسبة للتخزين والتحليل.*"[3]

الشكل 6-1: قدرات جهات إنفاذ القانون على جمع الأدلة الجنائية الإلكترونية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 110. (رقم=59)

بينما أفادت بعض البلدان توفُّر القدرة الاتحادية أو المركزية "*لدى أي معمل [جنائي] مركزي أو الوحدات الخارجية المسؤولة عن تحليل الخبرة للأدلة الإلكترونية التي جرى الحصول عليها في تحقيقات الشرطة*".[4] بينما أفادت غيرها من بلدان أخرى استخدام نهج موزع مع "*وحدات التحقيق الجنائي في جميع أنحاء البلد*"[5] التي "*تجري الفحوصات الجنائية الإلكترونية باستخدام أدوات التحقيق الجنائي المتخصصة ... المستخدمة بالنسبة للشبكات، ونظم الحاسوب، والهواتف المحمولة، وأجهزة التخزين.*"[6] وقد سلطت العديد من البلدان، خاصة الدول النامية، الضوء على نقص الموارد من أجل الحصول على معدات التحقيق الجنائي الفنية والتحديات التي تواجهها في تعيين الموظفين ذوي المهارات الكافية لإجراء التحقيقات ومعالجة الأدلة الإلكترونية. وقد أفادت إحدى البلدان في أفريقيا، على سبيل المثال، أنه "يتوفر عدد قليل من الفاحصين الجنائيين على المستوى الاتحادي، ولكن بما لا يكفي لخدمة البلد بالكامل، ولا يعمل إلا مختبر واحد".[7]

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 110.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 109.

[3] المرجع نفسه

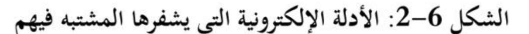
[4] المرجع نفسه

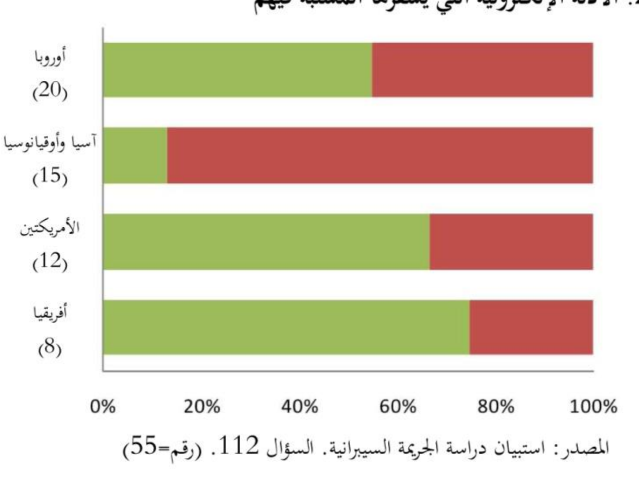
[5] المرجع نفسه

[6] المرجع نفسه

[7] استبيان دراسة الجريمة السيبرانية. السؤال رقم 111.

وقد أفاد عدد من البلدان أنه يعاني تشفير البيانات أثناء إجراء تحقيقات إنفاذ القانون وتحليل الأدلة الإلكترونية. وأفادت حوالي 60 إلى 80 في المائة من البلدان في جميع المناطق، باستثناء آسيا وأوقيانوسيا، أن الأدلة الجنائية كثيرا ما تشفر بمعرفة المشتبه فيهم.[1] بينما أفادت العديد من البلدان زيادة استخدام التشفير بمعرفة مرتكبي الانتهاكات. وقد رصد أحد البلدان أن "*بناء على نوع الجريمة، يصبح التشفير أكثر انتشارا.*"[2] ولم يكن هذا الرأي سائدا من قبل بأي حال من الأحوال. وقد أفادت إحدى بلدان أوروبا، على سبيل المثال، أن "*الأدلة التي يجري تجميعها نادرا ما تشفر مقارنة بكم البيانات المجمعة.*"[3] علاوة على ذلك، لا يتضح الأمر سواء كانت النسبة الأكبر من التشفير التي أبلغت عنها البلدان في آسيا وأوقيانوسيا نتيجة للاختلافات في استخدامات التشفير الكامنة التي يقوم بها المشتبه فيهم أو نتيجة لقدرات إنفاذ القانون على كشف المواد المشفرة وتحليلها.


الشكل 6–2: الأدلة الإلكترونية التي يشفرها المشتبه فيهم



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 112. (رقم=55)

وقد أشارت البلدان إلى "*عدم وجود طريقة بسيطة*" للتغلب على "*التحدي الشاق*" المتمثل في التشفير "*الذي يتطلب مساعدة وقدرة فنية متخصصة.*"[4] وقد أشارت بلدان عدة إلى عدم امتلاكها لسبل وأدوات التعامل مع مشكلة التشفير دون الحصول على المفاتيح من المشتبه فيه أو الاستحواذ عليها. وقد أفادت إحدى البلدان، على سبيل المثال، أنه: "*إذا خضع المشتبه فيه للتوقيف أو جرى التعرف عليه، يجب الحصول على مفاتيح فك التشفير من المشتبه فيه أثناء التحقيق.*"[5] وقد توفرت لدى بعض الاختصاصات علاجات قانونية لإجباره على التعاون.[6] إذا لم يفصح المشتبه فيه عن مفاتيح فك الشفرة، للمحققين الاستعانة ببرامج البرامجيات، أو اللجوء إلى

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 112.

[2] المرجع نفسه

[3] المرجع نفسه

[4] المرجع نفسه

[5] المرجع نفسه

[6] تنص لائحة قانون سلطات التحقيق لسنة 2000 في أحد بلدان أوروبا الشمالية، على سبيل المثال، على سلطة طلب الإفصاح عند إفصاح أحد المشتبه فيهم عن مفتاح حماية المعلومات التي في حوزته. وفي حال عدم امتثاله، لإخطار الإفصاح، يمكن أن يخضع للحبس أو الغرامة عند اتهامه. وعلى غرار ذلك، يسمح قانون الجرائم السيبرانية لسنة 2001 في أحد بلدان أوقيانوسيا للقاضي بإصدار أمر يطلب فيه من أحد الأشخاص تقديم أي معلومات أو مساعدة مقبولة وضرورية للسماح لمسؤول إنفاذ القانون بالوصول إلى البيانات المحتفظ بها في أي جهاز حساب آلي أو التي يجري الوصول إليها منه.

الخبرة الفنية، أو تقديم الأدلة الممكنة للمعامل الجنائية أو المختص لمحاولة فك التشفير. وقد ذكر أحد البلدان اللجوء إلى "*المختصين المعتمدين والبرامجيات المعتمدة*"[1] في جهود فك التشفير. وقد أشارت البلدان الأخرى إلى احتمال توقيف المشتبه فيه "*أثناء فتح الآلات وتشغيلها*"[2] عندما تكون البيانات غير مشفرة.

إضافة إلى التحديات التي تواجه التحقيقات الجنائية الرقمية في صورة تكنولوجيا التشفير، قد يستخدم مرتكبو الانتهاكات تقنيات "إخفاء المعلومات في الاتصال الإلكتروني" ("إخفاء" المعلومات). وهذا يتضمن إخفاء المعلومات والاتصالات داخل ملفات البريئة، مثل الصور البيانية، والمستندات، والعينات الصوتية، والتطبيقات. وتمثل ملفات الوسائط مضيفات مثلى لإخفاء المعلومات؛ لأنها عادة ما تكون كبيرة، وبالتالي لا تثير الشبهات على الفور. من وجهة النظر الجنائية، قد يجري التعرف على البيانات المخفية بمقارنة تدفقات ملفات وبيانات المشتبه فيه مع الأصول المعروفة. وقد ركز عدد من الدول المجيبة على الزيادة عامة في استخدام أساليب التشويش والتشفير. وقد أفادت إحدى بلدان الأمريكتين أن "المنظمات الجنائية تحاول إجراء تحقيقات صعبة بتخزين البيانات الجنائية في خوادم خارجية أو في نظم تخزين سحابية، واستخدام التشفير وغيرها من أساليب التشويش على البيانات."[3]

تمثل زيادة استخدام الحوسبة السحابية تحديات خاصة للأدلة الجنائية الرقمية. قد تصبح المعلومات التي يخزنها مرتكبو الانتهاكات عن بعد في الخدمات السحابية مرئية للمحققين أثناء البحث أو الفحص الجنائي، مثل التي تواجهها جلسات الإنترنت المباشرة على الأجهزة قيد التشغيل، أو من خلال الخدمات عن بعد المتاحة على أجهزة الهاتف الجوال المحتجزة. إضافة إلى الاعتبارات القانونية المتصلة بالوصول المباشر لإنفاذ القانون للمعلومات خارج حدود الدولة (التي جرت مناقشتها في الفصل السابع (التعاون الدولي)) يُعقِّد تخزين البيانات السحابية عملية التحقيق الجنائي للتعرف على المعلومات المخزنة إلكترونيا وتجميعها وتحليلها.[4] ويمثل احتمال وصول أحد مستخدمي السحابة إلى بيانات شخص آخر احتمالا بوجود المزيد من التحديات أمام صحة البيانات.

بمواجهة هذه التحديات، أفادت البلدان المجيبة باستخدام أساليب متنوعة لضمان الحفاظ على تكامل الأدلة الإلكترونية المجمعة خلال التحقيقات الجنائية الرقمية. وأشارت البلدان، على سبيل المثال، إلى استخدام التصوير الجنائي، واستخدام الإقرارات المشفوعة بيمين لإثبات صحة البيانات، قيم تجزئة التحقيقات الجنائية، استخدام أدوات حظر الكتابة، الحصول على بيانات الإنترنت من خلال لقطات الشاشة، أساليب التسمية والتوثيق والتعبئة والنقل المنتظمة، وختم صور التحقيقات الجنائية المسجلة على القرص البصري.[5] وبالنسبة للمعايير

---

[1] المرجع نفسه

[2] المرجع نفسه

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 85.

[4] Reilly, D., Wren, C., and Berry, T., 2011. Cloud computing: Pros and Cons for Computer Forensic Investigators. *International Journal Multimedia and Image Processing*, 1(1):26-34, 33.

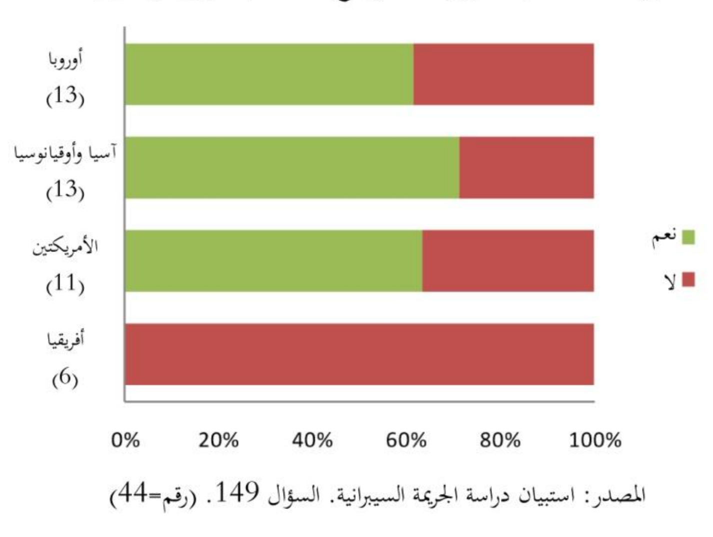
[5] استبيان دراسة الجريمة السيبرانية. السؤال رقم 111.

والمبادئ التوجيهية للتحقيقات الجنائية أشارت بضع بلدان إلى "دليل الممارسات الجيدة للأدلة الإلكترونية الحوسبية" لاتحاد كبار ضباط الشرطة.[1]

كما أفادت البلدان بعدد من الممارسات لتخزين الأدلة الإلكترونية لحمايتها من التدهور والتلف. وشمل هذا استخدام نسخ مطابقة عدة من أصل نسخة واحدة أساسية، وتخزين بيانات الحاسوب داخل شبكة التحقيقات الجنائية لتكنولوجيا المعلومات المخصصة في ظل الوصول المحدود، واستخدام المنشآت التي التحكم بالرطوبة ودرجة الحرارة والإشعاع الكهرومغناطيسي فيها، واستخدام الخزانات، واستخدام الأجهزة المقاومة للكهرباء الساكنة، واستخدام أقفال الأدلة المراقبة، واستخدام الحقائب المحكمة.[2]

إضافة إلى قدرة إنفاذ القانون في التحقيقات الجنائية الرقمية، من المهم أن يكون *للمدعين العامين* موارد كافية للتعامل مع الأدلة الإلكترونية وتحليلها. فالأدلة الإلكترونية التي لا تقدم في المحكمة ليس لها أي دور في الحكم العادل على المتهم. وتشير إجابات البلدان أن المدعين العامين لديهم مستوى من الموارد الخاصة بالتعامل مع الأدلة الإلكترونية يقل عن نظيره الخاص بإنفاذ القانون.[3] وقد علقت بعض البلدان، على أن المدعين كثيرا ما يعانون صعوبة في تفسير الأدلة الإلكترونية ويحتاجون مساعدة غيرهم من المختصين لتحديد الاتجاهات والوصول إلى معنى البيانات.[4] ولم يفد أي من المجيبين الأفريقيين بكفاية موارد المدعين العامين من أجل الحصول على الأدلة الإلكترونية – مع تسليط الضوء على إحدى المجالات الملحة للتركيز على المساعدة والدعم الفنيين.


الشكل 6–3: كفاية الموارد للتعامل مع الأدلة الإلكترونية وتحليلها



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 149. (رقم=44)

---

[1] أنظر http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 111.

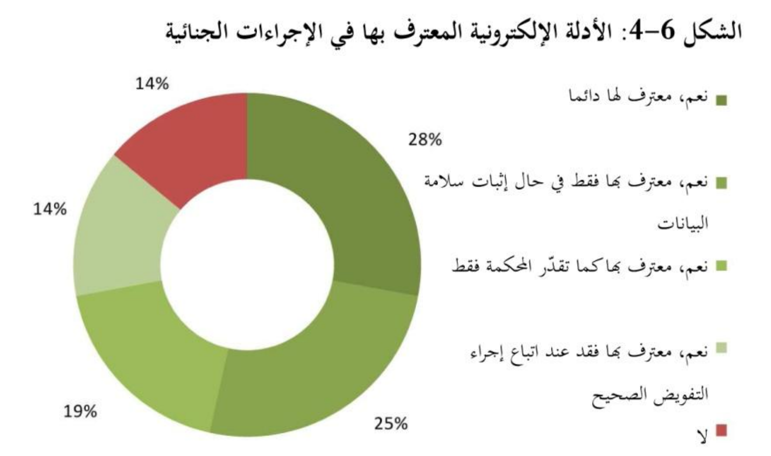
[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 149.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 149.

الأدلة الإلكترونية في الإجراءات الجنائية

أفادت أكثر من 85 في المائة من الدول المجيبة بأن الأدلة الإلكترونية معترف بها في الإجراءات الجنائية.[1] وقد أفاد عدد قليل من البلدان – معظمها في أفريقيا وآسيا – أن الأدلة الإلكترونية غير معترف بها. وقد أشر أحد بلدان أفريقيا، على سبيل المثال، أن الأدلة الإلكترونية "*غير منصوص عليها في القانون وبالتالي غير معترف بها*."[2] وفي هذه الحالة، يوجد عائق خطير أمام نجاح القضاء في الجريمة السيبرانية والجرائم التي تتضمن أدلة إلكترونية. وبالنسبة لهذه البلدان التي يعترف فيها بالأدلة الإلكترونية في العموم، تخضع هذه المقبولية لشروط، مثل تكامل البيانات، أو تقدير المحكمة، أو إجراءات التصديق، في حوالي 70 في المائة من البلدان.[3]

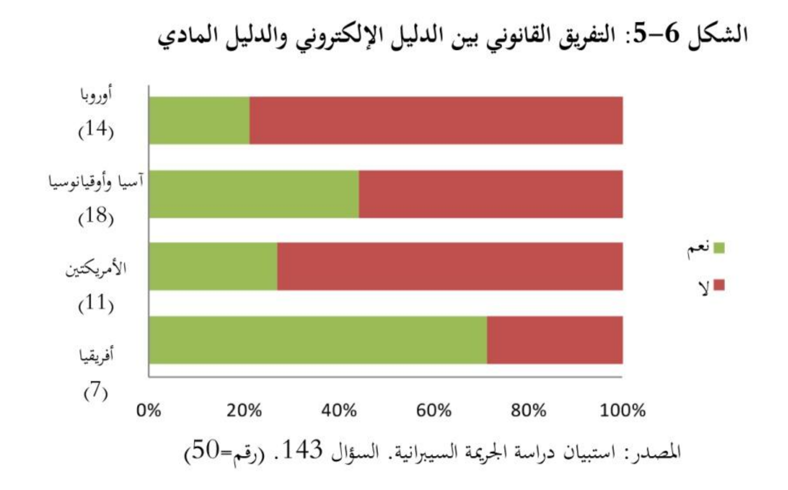
الشكل 6–4: الأدلة الإلكترونية المعترف بها في الإجراءات الجنائية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 144. (رقم=43)

وبرغم الاعتراف بالأدلة الإلكترونية في المحاكم الوطنية، أفادت إحدى البلدان بعدم الاعتراف بالأدلة الإلكترونية من *خارج* اختصاصها.[4] وفي حالة الجريمة عبر الوطنية، كالجريمة السيبرانية، يمكن لهذا القيد أن يؤثر على احتمال نجاح التقاضي. وقد أفاد عدد من البلدان أن قضايا

الشكل 6–5: التفريق القانوني بين الدليل الإلكتروني والدليل المادي



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 143. (رقم=50)

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 144.
[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 143.
[3] المرجع نفسه
[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 145.

المقبولية للأدلة الإلكترونية خارج الحدود كثيرا ما تثار بشأن أي الإجراءات التي اتبعت للمساعدة القانونية المتبادلة. وقد ركزت إحدى البلدان، على سبيل المثال، على أن "الأدلة الأجنبية المقدمة في الإجراءات الجنائية يجب أن تكون في صورة شهادة الشهود وأي مستند مرفق بهذه الشهادة، ويجب أخذ شهادة الشهود بعد حلف اليمين أو توقيع إقرار، أو في ظل الحيطة أو الحذر المقبول من المحكمة في البلد الأجنبي، أو في ظل الالتزام المفروض بقول الحق (سواء صراحة أو ضمنا)، أو بموجب قانون البلد الأجنبي، ويجب توقيع شهادة الشهود أو اعتمادها من القاضي أو المسؤول."[1] وفي العديد من الاختصاصات، كثيرا ما تحول هذه المتطلبات دون الاعتماد على الأدلة الإلكترونية خارج الحدود التي يجري الحصول عليها من خلال القنوات غير الرسمية من الشرطة إلى الشرطة في المحاكمات الجنائية.

وأفادت معظم البلدان التي تعترف بالأدلة الإلكترونية أنها تعاملها معاملة الأدلة المادية. ولكن أفاد ما يقل عن 40 في المائة من البلدان، وجود تفرقة قانونية بين الأدلة الإلكترونية والمادية.[2] وبينما تتعدد الأساليب، اعتبرت معظم البلدان أنه من الممارسات الجيدة عدم التفرقة، حيث يضمن هذا مقبولية الأدلة الإلكترونية بالإضافة إلى جميع أنواع الأدلة الأخرى. وبالنسبة للبلدان التي لا تفرق بين الأدلة الإلكترونية والمادية، أفاد العديد منها أن الأدلة الإلكترونية، على غرار مثيلاتها، "*يجب أن تكون: معترفا بها، ذات حجية، دقيقة، كاملة، ومقنعة لهيئة المحلفين*".[3] وقد كانت مقبولية الأدلة الإلكترونية بناء على القواعد العامة السارية على جميع الأدلة، بما فيها "*العناصر التي يجري الحصول عليها قانونا، مع احترام مبدأي وثاقة الصلة بالموضوع والوفرة.*"[4] وفي بضع بلدان يكون التقدير للمحكمة "*في تقرير مدى الاعتراف بالأدلة [الإلكترونية]*".[5]

وأفادت التقارير بإحالة الأدلة الإلكترونية إلى القضاء أو السلطات القضائية، واستخدامها في المحاكمات الجنائية بطرق شتى. وقد أفادت البلدان المجيبة كل الآتي: النقل المادي للحواسيب المحتجزة إلى المحكمة، واستخدام نسخ في المحكمة من بيانات الحاسوب المخزنة على القرص البصري، واستخدام النسخ المطبوعة للأدلة الإلكترونية المقدمة في مجلدات في المحكمة، وتقديم تقرير تحليلي للخبير وشهادته فقط أمام هيئة المحكمة (باستخدام بيانات الحاسوب التي لا تزال مخزنة).[6] وقد أفادت بضع البلدان، على سبيل المثال، "*أن الوثائق أو البيانات الإلكترونية يجب طباعتها قبل إمكانية قراءتها في الجلسة الرئيسة.*"[7] كما ركزت بعض البلدان على أنه "*لا يحال إلى المدعين*

[1] المرجع نفسه

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 143.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 143.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 144.

[5] المرجع نفسه

[6] المرجع نفسه

[7] المرجع نفسه

العامين إلا الجزء من الأدلة المجمعة وثيق الصلة بالموضوع – تخزن المواد والبيانات التي لا علاقة لها بالموضوع لدى الشرطة."[1]

كما قدمت البلدان تفاصيل عن عدد صيغ وسبل تقديم الأدلة الإلكترونية بالمحكمة. وشمل هذا شهادة الشهود التي يقدمها ضباط الشرطة، شهادة الشهود التي يقدمها أخصائيو الطب الشرعي، بما في ذلك تقديم المعلومات الرقمية على أجهزة العرض والشاشات العريضة، والمطبوعات التي تنص على الأشياء والوثائق والصور والسجلات ولقطات الشاشة.[2] وركزت إحدى البلدان في آسيا على اللجوء إلى تقارير الخبراء، بالإشارة إلى أن "*التقارير المكتوبة عادة ما تقدم مرفقة بتفسيرات بشأن البيانات الفنية*." وقد أشارت غيرها من البلدان إلى عرض الأدلة الإلكترونية على شاشات الحاسوب: "في إحدى قضايا الحاسوب المعقدة، أثبت استخدام جهاز العرض لتقديم الأدلة فاعليته في تقديم المعلومات من المدعي العام إلى المحكمة."[3]

وأفادت بلدان أخرى بسبل متعددة لعرض الأدلة. فقد أشارت إحدى البلدان في أوروبا، على سبيل المثال، أن عرض الأدلة الإلكترونية بالمحكمة "*يعتمد على حالة الأدلة ومكانها. [يجوز تقديم الأدلة الإلكترونية في صورة] مطبوعات ورقية، وسائط رقمية (أقراص صلبة، أقراص مضغوطة، أقراص الفيديو الرقمي، الذاكرة الوميضية)، العروض على الحواسيب الشخصية والحواسيب المحمولة، العروض عن بعد، الوصول [الحي] في بعض الحالات النادرة*." وقد سلطت بعض البلدان الضوء، رغم ذلك، على أن قاعات المحاكم لم تكن مجهزة لاستخدام التكنولوجيا في المحاكمات الجنائية، حيث أشارت إحدى بلدان الأمريكتين، على سبيل المثال، أن "المحاكمات الإلكترونية لا تزال غير شائعة. فليست جميع قاعات المحاكم موصلة لغرض السماح [للدولة] بعرض القضايا إلكترونيا. وحاليا، يجب [على الدولة] أن تحصل على موافقة القضاة وهيئة الدفاع لاستخدام التكنولوجيا في قاعة المحكمة."[4]

وقد أفادت بضع البلدان بوجود قوانين خاصة بالأدلة تحكم الأدلة الإلكترونية. وبالنسبة لهذه البلدان، يجوز اعتبار المجالات التي تعني بها القوانين مثل الافتراضات القانونية بشأن ملكية البيانات والوثائق الإلكترونية وتأليفها، إضافة إلى الظروف التي وقعت فيها الأدلة الإلكترونية على أنها موثوق بها.[5] وقد قدمت بلدان أخرى معلومات بشأن طريقة تفسير القواعد "التقليدية" للأدلة في سياق الأدلة الإلكترونية. وقد أوضحت إحدى بلدان أوقيانوسيا، على سبيل المثال، كيفية تطبيق قاعدة "الإشاعات" على الأدلة الإلكترونية في اختصاصها: "*بالنسبة للأدلة الإلكترونية تحديدا، لا تسري قاعدة الإشاعات إذا كانت المعلومات الواردة في الأدلة الإلكترونية متعلقة*

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 143.
[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 150.
[3] المرجع نفسه
[4] المرجع نفسه
[5] استبيان دراسة الجريمة السيبرانية. السؤال رقم 147.

باتصال محول بين الحواسيب واعترف به من أجل تحديد المرسل والمرسل إليه وتاريخ التحويل وموعده."[1] وقد أشار بلد آخر إلى وجود *"الافتراض العام"* حيث إنه *"متى قدمت أدلة صادرة عن آلة أو جهاز آخر، إذا كان الجهاز هو المستخدم على النحو الصحيح في الحصول على هذه النتيجة عادة، فيعتبر أن الجهاز كان يعمل على نحو صحيح عند تكوينه للدليل."* [2]

وأخيرا، فقد نوّهت البلدان إلى *الطرق* التي يمكن بها استخدام الأدلة الإلكترونية لإقامة صلة بين العمل الإجرامي ومرتكب الجريمة المحدد. إن طبيعة الجريمة السيبرانية تعني أنّ جهاز وساطة، في شكل نظام الحاسوب، عادة ما يكون قائما بين الجاني والمجني عليه – مما يؤدي إلى تحديات في عزو الأعمال إلى أشخاص محددين. أما في الحالات التي يتم فيها محاكمة المتهم، على سبيل المثال، للاستيلاء على المحتوى غير القانوني للحاسوب، فيجب إثبات أن المحتوى قد تم وضعه عن قصد على الجهاز من قبل المدعى عليه، وليس من قبل شخص آخر عن طريق الوصول إلى الجهاز. وفي هذا الصدد، علّق بلد واحد بما يلي: *" تكون الأدلة الظرفية في كثير من الأحيان الوسيلة الوحيدة التي يمكن من خلالها تحديد هوية المتحدث أو المتصل. وقد أثبتت الأساليب التاليةَ جدارتها: إثبات ملكية جهاز الاتصال (الحجز وفق التوقيف أو تنفيذ الأمر)، ومعلومات المشترك، والرصد (بناء على إذن من المحكمة عند اللزوم)، تحليل محتوى الاتصال وفحص الطب الشرعي لجهاز الاتصال."* [3] في حين نوّه بلد آخر بما يلي:"عادة ما تكون هناك *مجموعات متعددة مختلفة من الأدلة الإلكترونية التي يجب جمعها سويّا لوضع المشتبه فيه وراء جهاز إليكتروني في وقت معين ومكان محدد."*[4]

كما أشارت معظم البلدان إلى عدم وجود خطوات محددة أو معايير معينة لإثبات الرابط. إضافة إلى ذلك، أشارت الدول إلى تنوع التقنيات التقليدية والسيبرانية المحددة "لربط الأدلة الإلكترونية بنظام حاسوب تحت سيطرة المدعى عليه، أو الذي له حق الدخول إليه. *"تطبيق تقنيات معيار ثبوت الأدلة القياسية بما في ذلك الحافز والفرصة والأدلة الداعمة غير الإلكترونية وضبط الأدلة ودليل الحالة العقلية والأدلة التي تدعم استبعاد الآخرين."* [5]

وإجمالا، نوهت البلدان المجيبة عن الاستبيان بشكل عام عن قدر كبير من المعرفة المتراكمةِ في مجال تحديدِ وجمع وتحليلِ وعرض الأدلة الإلكترونية. كما تم تسليط الضوءِ على الممارسات الجيدة في هذا المجال ليس من جانب البلدان المتقدمة فحسب، بل من جانب العديد من البلدان النامية أيضا– في إشارة إلى زيادة مستويات الحوار العالمي ونشر المعايير التقنية في مجالات الأدلة الإلكترونية. ليس ذلك فحسب، بل إن العديد من المؤسسات في البلدان النامية — بما في ذلك سلطات إنفاذ القانون والسلطات القضائية – سلّطت الضوء على نقص كبير في

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 146.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 143.

[56] استبيان دراسة الجريمة السيبرانية. السؤال رقم 148.

[4] المرجع نفسه

[5] المرجع نفسه

القدرات والموارد للتنفيذ الكامل لمثل هذه المعايير. بالإضافة إلى ذلك تمثّل العقبات القانونية، في القليل من البلدان، مثل عدم قبول كافة الأدلة الإلكترونية وعدم قبول الأدلة الإلكترونية خارج الحدود الإقليمية عقبات خطيرة أمام مقاضاة أفعال الجريمة السيبرانية.

3-6 الجريمة السيبرانية ونظام العدالة الجنائية في الممارسة

الاستنتاجات الرئيسية:

- نوه المدعون العامون إلى سلسلة من التحديات التي تواجه المحاكمة الناجحة للجريمة السيبرانية ، بما في ذلك كفاية الأطر القانونية والصعوبات في عزو الأفعال إلى أفراد والتأخير الناجم عن إجراءات التعاون الدولي وتحديات الإثبات
- تنعكس مثل هذه التحديات في الإحصاءات المتوفرة عن نسبة المشتبه فيهم في الشروع في أعمال مسجلة لدى الشرطة وتدابير "الاستنزاف" التي تقارن عدد الإدانات مع عدد الأعمال المسجّلة

يوسّع هذا القسم النقاش من الطب الشرعي والأدلة الإلكترونية إلى تطبيق نظام العدالة الجنائية، ككل، في حالات الجريمة السيبرانية. كما يناقش التحديات والممارسات الجيّدة التي نوه إليها المدعون العامون والمحاكم، ويحدد التأثير المحتمل لهذه المحاكمات والإدانات لمرتكبي الجريمة السيبرانية.

التحديات القضائية والممارسات الجيدة

حددت البلدان المجيبة عن الاستبيان الممارسات القضائية الجيدة والتحديات من خلال عملية العدالة الجنائية، من تناول القضية وحتى البت النهائي فيها. كما اقترحت إحدى البلدان، على سبيل المثال، مجموعة شاملة من الممارسات الجيدة في مجالات إدارة القضايا والإفصاح عن الأدلة وتقديم الأدلة في المحاكمة وهي كما يلي: "*1) التعاون والتواصل المبكر مع المحققين والعاملين في تكنولوجيا المعلومات والمساعدين القانونيين ومحامي الدفاع. 2) مخاطبة حماية مراقبة الجودة، على سبيل المثال، قواعد العمل. 3) التحقيق الجردي والإفصاح عن القائمة. 4) تحديد شاهد خبير قادر على الشهادة في قضايا مراقبة الجودة مثل اكتمال وسلامة قاعدة بيانات المحاكمة. 5) ضمان توافق وتبادلية أنظمة الحاسوب الشرطية والحكومية. 6) التقابل والتشاور المبكر مع محامي الدفاع في القضية. 7) تجنب خلط الوسائل. 8) القدرة على مواجهة الإفصاح. 9) التفكير في البيانات الفوقية من بداية والتماس المساعدة والدعم من الخبراء. 10) التأكد من أن الوثائق الإلكترونية قد تم تحريرها بشكل صحيح. 11) اختيار الأداة الإلكترونية الصحيحة لتتناسب مع نوع الأدلة التي ستقدم في المحاكمة. لا يتناسب*

حجم واحد مع الكل. 12) الحصول على إذن القاضي. 13) تحديد معروضات المحاكمة في وقت مبكر واختبار التجهيزات في المكتب أو قاعةِ المحكمة، بالإضافة إلى وضع الخطة الاحتياطية والاستعداد التام." [1]

تتعلق العقبات المنوّهِ إليها والتي تعيق المحاكمة الناجحة عموما بكفاية الإطار القانوني وتحديد المشتبه فيهم وتوافر الأدلة وتأويلها بالإضافة إلى الإجراءات المناسبة للتعامل مع الأدلة.

أما فيما يتعلّق بالتشريع للسلطات الإجرائية (التي تم مناقشتها في الفصل الخامس (إنفاذ القانون والتحقيقات))، فقد سلّطت البلدان المجيبة عن الاستبيان الضوء، على سبيل المثال، على *" عدم وجود إطار قانوني" و "عدم وجود تشريع إجرائي" و "عدم وجود سلطات التحقيق المناسبة التي لا تمس الحق في الخصوصية وحرية التعبير بطريقة مفرطة" بالإضافة إلى عدم وجودِ "تشريع محدد بشأن حماية الخصوصية"* [2] والذي يتسبب في تعقيد التحقيقات وتأخيرها.

وقد حدد المدعون العامون أيضا التحدي الذي تمت مناقشته في القسم السابق من هذا الفصل في عزو أدلة عمل ما إلى فرد. فقد نوّه بلدٌ واحد، على سبيل المثال، إلى أن *"إسناد الجريمة في العموم هو الجزء الأصعب في تحقيقات الجريمة السيبرانية، ولذا فهنا تكمن العقبة العملية التي تعيق المحاكمة الناجحة"* [3] كما سلّط المدعون العامون من البلدان المجيبة عن الاستبيان المزيد من الضوءِ على التحديات في القضايا ذوات البعد الخارجي، بما في ذلك *"صعوبة الحصول على الأدلة التي تتطلب تعاونا دوليّا من البلدان الأخرى" و "والتأخير في التحقيق والمقاضاة في الجريمة السيبرانية"* نتيجة لعمليّات التعاون الدولية الرسمية مثل المساعدة القانونية المتبادلة. [4]

تم التنويه إلى قضايا الإثبات كحواجز رئيسية تعيق المحاكمة الناجحة، بما في ذلك *"الحجم الكبير من الأدلة" و "الفترة الوجيزة من الزمن التي يقوم فيها مقدمو الخدمات بتخزين المعلومات اللازمة لأغراض التحقيق" و "الحفاظ على سلامة الأدلة الإلكترونية من وقت الحجز إلى نقطة الانتهاء من القضية" بالإضافة إلى "الإخفاق في إنشاء سلسلة من مسؤوليات الأدلة، وعدم وجود مرافق التخزين المناسبة للحفاظ على الأدلة."* [5] *"إن تقديم الأدلة على الجريمة السيبرانية ما يزال تحديا أمام المحكمة" و "عدم سلامة الأدلة من سوء التعامل معها من قبل إنفاذ القانون"* [6] تم تحديدها أيضا كأداة طعن خاص من قبل العديد من البلدان.

وقد عزّزت البلدان بشكل مستمر من أهمية جمع الأدلة وعرضها. كما أن"وجود علاقات عمل وثيقة داخل فريق القضاء بين المدعي العام والمحقق تثمرُ في جمع كافة الأدلةِ ذات الصلة الموثّقة بشكل صحيح" [7] وهو

61 استبيان دراسة الجرائم السيبرانية السؤال رقم 142.

2 المرجع نفسه

3 المرجع نفسه

4 المرجع نفسه

5 المرجع نفسه

6 المرجع نفسه

7 استبيان دراسة الجريمة السيبرانية السؤال رقم 142.

شيءٌ لا غنى عنه لتحقيق النجاح في الملاحقة القضائية. "كما يجب مصادرة الأجهزة، التي توجد فيها البرامج المناسبة، من المتهمين في أسرع وقت ممكن وبصورة قانونية....يليها التقييم السريع من قبل فريق مدرب تدريبا خاصا وذوي مهارة عالية أو متخصصين من الخارج."[1] "التحديد المنفصل وتتبع كافّة الوثائق والصور المتعلقة بالحاسوب"[2] "وسلسلة واضحة من مسؤوليات الأدلة المعروضة"[3] "وتطوير السياسات في العلاقة مع عرض الأدلة في المحكمة بناء على نجاح العروض السابقة"[4] كانت مكونات هامة للمحاكمات الناجحة والإدانات. وأخيرا، "فإن عدم وجود السلاسة المحسوسة في المجتمع القانوني فيما يتعلّق بالمفاهيم التكنولوجية وكيفية تأثيرها في إقامة العدالة"[5] "وفهم الأدلة الرقمية من قبل مأموري الضبط القضائي"[6] تم التنويه إليها كعقبات إضافية تعيق المحاكمة الناجحة والإدانة في قضايا الجريمة السيبرانية.

كما تم تحديد التدريب الإضافي والموارد كتحديات بما في ذلك "التوجيه الأفضل للمحاكم على كافة المستويات من خلال تلخيص (ومشاركة) الخبرة القضائية للسماح لمعايير التحديد والتنظيم في قضايا حماية نظام معلومات الحاسوب"[7] فقد سلّطت إحدى البلدان الضوء على "أنه من المهم والحاسم لحسن إدارة حالات الجريمة السيبرانية أن تمتلك المحاكم الوطنية موارد ماليّة كافية للحصول على المعدّات التقنيّةِ اللازمة."[8] ضرورة الشراكة بين القطاعين العام والخاص مع "مقدمي خدمات الوصول إلى الإنترنت ومقدمي خدمات استضافة المواقع بالإضافة إلى مقدمي الخدمات الأخرى"[9] وشركات البنوك والاتصالات تم التنويه إليها أيضا كطريقة مثمرة لتعزيز جمع الأدلة.

فعالية نظام العدالة الجنائية ونتائجه

إنّ الأهداف الرئيسية لاستجابة العدالة الجنائية، في أي جريمة، هي تحقيق مجرد النتائج للجناة والضحايا، إلى جانب الردع المحدد وإعادة التأهيل وإعادة الإدماج الاجتماعي للمجرمين المدانين واتجاه الردع العام للجناة المحتملين.[10] ويكمن التحدي الأصعب في قياس مدى "كفاءة" أو "فعّالية" تحقيقِ تلك الأهداف. تتراوح التدابير من معدلات "الاستنزاف" التي توفر المعلومات عن أعداد الأشخاص المشتبه فيهم والمحاكمين والمدانين من قبل نظام العدالة الجنائية بارتكاب جرائم محددة إلى تدابير تتسم "بدقة التوقيت" للفصل في القضية "الردع العقابي"

---

1 استبيان دراسة الجريمة السيبرانية السؤال رقم 183.

2 استبيان دراسة الجريمة السيبرانية السؤال رقم 142.

3 المرجع نفسه

4 المرجع نفسه

5 استبيان دراسة الجريمة السيبرانية السؤال رقم 141.

6 المرجع نفسه

7 استبيان دراسة الجريمة السيبرانية السؤال رقم 142.

8 استبيان دراسة الجريمة السيبرانية السؤال رقم 183

9 المرجع نفسه

10 Albanese, J.S., 2012. Criminal Justice. 5th edn. Upper Saddle River: Prentice Hall

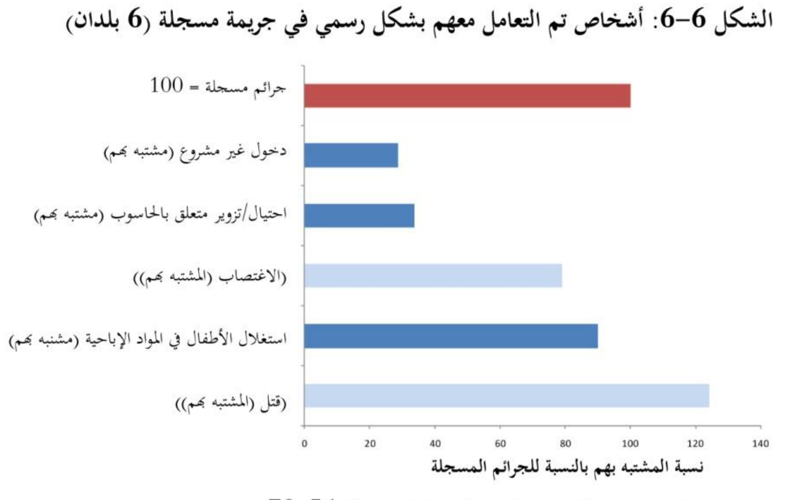
و"معاودة ارتكاب الجريمة".[1] وعلى الرغم من أن كافة هذه التدابير قد تم التنويه إليها في العموم إلا أنه ينبغي ملاحظة أنها لا تمثل مؤشرات مباشرة "لجودة" العدالة، ومن الممكن أن تتأثر بشكل كبير بسبب الاختلافات في آليات نظام العدالة الجنائية مثل تطبيق قواعد العد المشبوهة، والحدود المطبّقة في تسجيل الحالات أو تدخّل الإدعاء العام في مرحلة التحقيق الأولي.

إضافة إلى ذلك ومن أجل مزيد من الفهم لاستجابة نظام العدالة الجنائية للجرائم السيبرانية فقد طلب استبيان الدراسة من البلدان أن تقدم تقريرا بالإحصاءات المتوفرة عن عدد الجرائم السيبرانية المسجلة وعدد الأشخاص المشتبه فيهم (أو "الذين تم التعامل معهم رسميا من قبل الشرطة") في الجريمة السيبرانية فضلا عن عدد الأشخاص الذين تمت محاكمتهم أو إدانتهم في إرتكاب جريمة سيبرانية.[2]

وكما هو ملاحظٌ في الفصل الثاني (الصورة العالمية) فقد تم العثور على تقارير إحصاءات شرطية لا تشكّل أساسا قويّا للقياس النسبي الدولي لاتجاهات الجريمة السيبرانية.[3] مع ذلك، قد يسمح إنفاذ القانون وإحصاءات العدالة الجنائية في كل بلد على حدة للحالة والمشتبه بالتلاعب في الحسابات لتلك الدولة، حيث كانت أرقام القضايا ليست بالقليلة، ويمكن حصر الآثار (مثل القضايا التي تم ترحيلها من سنة واحدة إلى أخرى) من عام إلى عام.

بشكل عام، كانت البلدان المجيبة عن الاستبيان قادرة على توفير عدد قليل نسبيا من إحصاءات إنفاذ القانون والعدالة الجنائية وإحصاءات المحاكم. ومع ذلك، كان من الممكن بالنسبة لمجموعة مكونة من ست بلدان، معظمها في أوروبا، حساب

الشكل 6-6: أشخاص تم التعامل معهم بشكل رسمي في جريمة مسجلة (6 بلدان)



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 54-70.

1 أنظر على سبيل المثال، Harrendorf, S., Smit, P., 2010 . سمات نظم العدالة الجنائية-الموارد والأداء و punitivity . في: المعهد الأوروبي لمنع ومكافحة الجريمة التابع للأمم المتحدة (HEUNI) 2010. الإحصاءات الدولية بشأن الجريمة والعدالة Helsinki .

2 استبيان دراسة الجريمة السيبرانية. السؤال رقم 54-70 و 121-137 و 165-181.

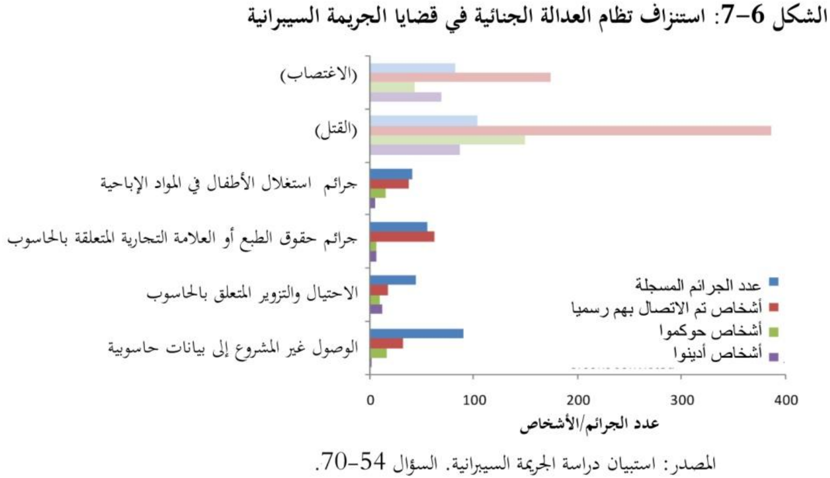
3 أنظر الفصل الثاني (الصورة العالمية)، القسم 2-1 قياس الجريمة السيبرانية، والقسم 2-3 مرتكبي الجرائم السيبرانية، وملامح "الجاني النموذجي"

متوسط عدد الأشخاص الذين تم التعامل معهم بشكل رسمي من خلال سلطات إنفاذ القانون في جرائم تم تسجيلها، بخصوص ارتكاب أفعال الجريمة السيبرانية، من الوصول غير المشروع والاحتيال والتزوير المتعلق بالحاسوب وجرائم استغلال الأطفال في مواد إباحية.

يبين الشكل 6-6 هذه النتائج بجانب المشتبه فيهم إلى نسب جريمة الاغتصاب والقتل في نفس الدول الست.[1] هناك فرق كبير بين جرائم استخدام الأطفال في المواد الإباحية وجرائم الحاسوب الأخرى من الوصول غير المشروع والاحتيال أو التزوير. فنسبُ المشتبه فيهم في ارتكاب جرائم استخدام الأطفال في المواد الإباحية مماثلةٌ لنسب الجرائم "التقليدية". أما بالنسبة لمرتكبي جرائم الوصول غير المشروع والاحتيال والتزوير المتعلق بالحاسوب فنسبتها أقل من ذلك بكثير متمثّلة في نحو 25 من حالات الاشتباه المسجلة لكل 100جريمة.

قد يكون هذا مؤشرا على عدد من العوامل، بما في ذلك الاختلافات في قدرات التحقيق للشرطة في الجريمة السيبرانية المختلفة، والاختلافات في تركيز تحقيقات الشرطة والتغيرات في النقطة التي تم تسجيل أفعال الجريمة السيبرانية المختلفة فيها كجرائم لأهداف إحصائية. بالإضافة إلى ذلك، قد يكشف النموذج عن اختلافات حقيقية كامنة في الخطوات، والقدرات، التي يتخذها مرتكبو الجريمةُ لإخفاء النشاط الإجرامي وتجنب الكشف من قبل تحقيقات إنفاذ القانون.

الشكل 6-7: استنزاف نظام العدالة الجنائية في قضايا الجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 54-70.

في حين أنه يمكن حساب نسب المشتبه بهم إلى الجريمة كمتوسط لعدد البلدان، وقدّمت إحصاءات كافية لحساب كامل "الجريمة إلى الإدانة" معدل الاستنزاف من دولة واحدة فقط ردا على استبيان الدراسة. يوضح الشكل 6-7 عدد الجرائم المسجلة لدى الشرطة، والأشخاص الذين تم التعامل معهم بشكل رسمي، والأشخاص الذين تمت محاكمتهم والمدانين في ارتكاب أربعة أعمال جرائم سيبرانية في بلد واحد يقع في أوروبا الشرقية، بجانب البيانات المعادِلة عن الجرائم "التقليدية" مثل الاغتصاب والقتل. وتؤكّد البيانات صورة لعدد أكبر من المشتبه بهم في جريمة مسجّلة من جرائم استخدام الأطفال في المواد الإباحية أكثر من أعمال الجريمة السيبرانية. ويتكرر هذا النمط في جريمة متعلقة بمحتوى آخر وهي جرائم حقوق الطبع والنشر أو العلامات التجارية المتعلقة بالحاسوب. وبشكل عام، فإن كافة الجرائم

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 54-70؛ استقصاء الأمم المتحدة لاتجاهات الجريمة وعمليات نظم العدالة الجنائية، آخر سنة متاحة.

السيبرانية تعرض أشخاصا تمت محاكمتهم أو إدانتهم في ارتكاب جريمة سيبرانية أقلّ من الجرائم التقليدية. وبالنسبة للبلد الذي أرسل تقريره فإن إدانات الجريمة السيبرانية تمثل، في المتوسط، 10 في المائة من الجرائم المسجّلة لدى الشرطة مقارنة بنحو 80 في المائة من جرائم الاغتصاب والقتل.

ويظهر النموذج أن العدد الكبير من تحدّيات مقاضاة الجريمة السيبرانية التي نوّهت إليها البلدان المجيبة عن الاستبيان قد ثبت صحتها في واقع انخفاض معدلات الإدانة للجرائم السيبرانية – على الأقل بالنسبة لهذا البلد النموذج. كما نوقش في القسم التالي من هذا الفصل، في العديد من البلدان النامية، مسألة أن مقاضاة الجريمة السيبرانية تواجه تحديا ليس في جمع الأدلة عبر الوطنية والتشويش من طرف الجاني فحسب، بل أيضا في القدرات النيابية والقضائية ومحدودية الاختصاصات.

4-6 قدرة العدالة الجنائية

الاستنتاجات الرئيسية:

- تُعد مستويات التخصصات القضائية في الجريمة السيبرانية أقل مقارنة بسلطات إنفاذ القانون. وقد وضعت حوالي 60 في المائة من كافة الدول المجيبة عن الاستبيان هياكل قضائية متخصصة للجريمة السيبرانية
- وأظهرت البلدان المتقدمة وجود مستويات للتخصصات القضائية أعلى من البلدان النامية
- لوحظ في 60 في المائة من البلدان الأقل تقدما أن المدعين العامين المتخصصين إما يتمتعون بالمهارات الأساسية في تكنولوجيا المعلومات والمعدات الحاسوبية المتوسطة أو لا يتمتعون بذلك على الإطلاق
- وأظهرت المحاكم مستويات أدنى للتخصصات المتصلة بالجريمة السيبرانية، حيث أن 10 في المائة من البلدان تبلغ عن الخدمات القضائية المتخصصة. ويتولّى النظر في الأغلبية العظمى من قضايا الجريمة السيبرانية قضاة غير متخصصين لا يتلقون في 40 في المائة من البلدان المجيبة عن الاستبيان أي نوع من التدريب المتصل بالجريمة السيبرانية

وعلى غرار ما هو الحال عليه في الجريمة السيبرانية والتحقيقات القائمة على الأدلة الإلكترونية التي تستلزم وجود تخصص في إنفاذ القانون، فإن القضاء وإصدار الأحكام القضائية المتصلة بقضايا الجريمة السيبرانية تنادي أيضا بوجود تخصص في نظام القضاء الجنائي. ويستلزم مثل هذا التخصص وجود موظفين لهم دراية بالمفاهيم الخاصة بالحاسوب والإنترنت، ومعرفة بالأطر التشريعية للجرائم السيبرانية، والقدرة على تقديم الأدلة الإلكترونية وفهمها من أجل إقامة الحجة عند المحاكمة.

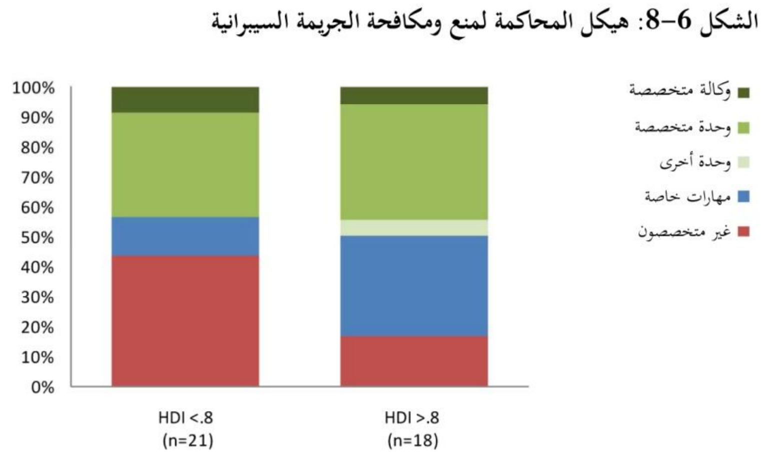
ويعرض هذا القسم المعلومات التي تقدمها البلدان بشأن قدرة المدعي العام والمحاكم على المقاضاة وإصدار أحكام قضائية تتعلق بالجريمة السيبرانية. وكما ذكر في الفصل الخامس (إنفاذ القانون والتحقيقات) تمتلك القدرة المؤسسية عدد من العناصر تشمل القدرات التشغيلية والاستراتيجية والمهارات الفنية للموظفين وكفاءة الموظفين والموارد بالإضافة إلى درجة التخصص. وتنطبق النقطة التي تم تناولها في الفصل الخامس، المتعلقة بالاحتياج المتزايد لكافة موظفي إنفاذ القانون للتعامل بشكل روتيني مع الأدلة الإلكترونية وجمعها، بالتساوي على القضاة والمدعين العامين إذ كلما تقدم العالم الرقمي، يصبح من الصعب تصوُّر البت في أي جريمة دون تقديم الأدلة الإلكترونية وأخذها في الاعتبار.

التخصص التنظيمي

وتؤكد البلدان المجيبة عن الاستبيان الخاص بهذه الدراسة أن درجة تخصص الجريمة السيبرانية التنظيمي مقارنة بسلطات الإدعاء أقل بكثير من تلك التي وردت فيما يخص سلطات إنفاذ القانون. حيث أن أكثر من 90 في المائة من البلدان أفادت بوجود نوع من التخصص في الجريمة السيبرانية في إنفاذ القانون، وتنخفض هذه النسبة لحوالي 60 في المائة بالنسبة لسلطات الإدعاء في جميع البلدان المجيبة عن الاستبيان.[1] وعلى الرغم من هذا، يخفي هذا الرقم اختلافات جوهرية وفقا لمستويات التنمية في البلد.

وأفادت حوالي 80 في المائة من البلدان الأكثر تطورا وجود بعض أنواع التخصصات القضائية في الجريمة السيبرانية. وتمتلك حوالي نصف هذه البلدان وحدات متخصصة بينما يمتلك النصف الآخر وكالة متخصصة ووحدة متخصصة (مثل ما يتعلق بالجريمة المنظمة) أو موظفين متخصصين غير منظمين في وحدة منفصلة. وفي المقابل، أفاد أقل من 60 في المائة من البلدان الأقل تطورا وجود تخصص قضائي في الجريمة السيبرانية، وفي معظمها تعتبر درجة التخصص في مستوى الوحدة المتخصصة.

الشكل 6–8: هيكل المحاكمة لمنع ومكافحة الجريمة السيبرانية



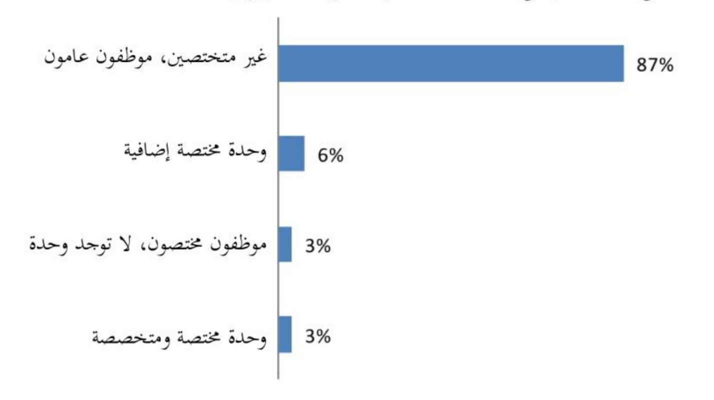
المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 157. (رقم=41)

بالنسبة للبلدان المتقدمة التي تبلغ عن التخصص التنظيمي، يشير العديد إلى وجود قسم متخصص أو وحدة متخصصة في الاتحاد داخل وزارة العدل أو وكالة القضاء الوطنية تشرف على المتخصصين والوحدات المتخصصة وتنسيقها ودعمها بتكرار في المكاتب المحلية والميدانية. وأبلغت بعض الدول عن وجود دعم فني

[1] استبيان دراسة الجريمة السيبرانية، السؤال 157.

وتحقيقي من فريق متخصص من محققي الشرطة ومهندسي الحاسوب والمدعين العامين الذين يحققون في الجريمة السيبرانية.[1] وفي بعض الحالات تمتلك هيئات القضاء الفردية كفاءات خاصة للتعامل مع مجموعات بارزة من الإجراءات المتصلة بجرائم المعلومات والاتصالات وفي الجريمة السيبرانية بالمعنى الدقيق للكلمة. وأشارت بلد متقدمة أخرى *"أنه يوجد بعض الاختلافات ولكن يمتلك عدد قليل من المكاتب المحلية أفرقة متخصصة لحماية الأطفال من الاستغلال عبر الانترنت"* .[2]

الشكل 6–9: هيكل المحكمة لقضايا الجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 186. (رقم=31)

في الدول الأقل تطورا لم يتم إجراء استعدادات كافية. وأفادت دولة في أفريقيا أنها كلفت وحدتها التي أنشئت حديثا مع القضاء بالإضافة إلى تقديم المشورة بشأن التشريعات والسياسات، وتقديم المساعدة الفنية للمدعين العامين الآخرين ووكالات إنفاذ القانون، ولكن باعتبارها وحدة جديدة ينبغي لها تلبية احتياجات التدريب والمعدات[3]. وأفيد "بوجود مساحة كبيرة للتحسين" في بعض الحالات. وأفادت بلاد في أفريقيا بعدم وجود مدعين عامين مخصصين للتعامل مع حالات الجريمة السيبرانية، حيث يتطلب من أي مدعي عام بالتعامل مع الجريمة السيبرانية حتى هؤلاء الذين لم يتلقوا أي تدريب يخص الجريمة الإلكترونية.[4]

أشار عدد قليل من البلدان التي ليس لديها هياكل قضائية إلى وجود خطط لإنشاء هياكل قضائية للجريمة السيبرانية. تضمنت هذه الخطط مقترحات "لإنشاء عدد من الوحدات المتخصصة" "وخطط لإنشاء أفرقة عمل في المدن الكبرى التي لا تمتلك حاليا هياكل قضائية متخصصة.[5] بلد واحد في أوروبا يتصور إنشاء "وحدات مستقلة في مكاتب المدعين العامين مع مقدار كبير من الأنشطة وفي المكاتب المتبقية لجمع المدعين العامين المتخصصين في الإنترنت مع الأنواع الأخرى من الوحدات المتخصصة.[6] ولم تذكر بلدان أخرى وجود خطط للوحدات المتخصصة على الرغم أن بعض هذه البلدان أفادت بوجود تقارير لدمج المتخصصين الإلكترونيين في وحدات مختصة أخرى.

---

[1] استبيان دراسة الجريمة السيبرانية، السؤال 157.

[2] المرجع نفسه

[3] المرجع نفسه

[4] استبيان دراسة الجريمة السيبرانية، السؤال 160.

[5] استبيان دراسة الجريمة السيبرانية، السؤال 157.

[6] المرجع نفسه

وأظهرت هياكل المحاكم درجة أقل من التخصص وقد أفاد حوالي 10 في المائة من كافة البلدان المجيبة عن الاستبيان بوجود درجة معينة من تخصص الجريمة السيبرانية في المحاكم. وأفاد 3 في المائة من البلدان المجيبة عن الاستبيان بوجود وحدة قضائية متخصصة في الجريمة السيبرانية. وأفاد 6 في المائة من البلدان بوجود نوع مختلف من الوحدة القضائية المتخصصة مثل محاكم الجرائم التجارية. وأفادت 3 في المائة من البلدان بوجود الإشراف القضائي على حالات الجريمة السيبرانية من خلال موظفين قضائيين مختصين.

وأشارت القليل من البلدان إلى وجود خطط جارية سواء من خلال التشريعات أو التدابير الإدارية لإنشاء محاكم وهيئات متخصصة في الجريمة السيبرانية. وبوجه عام، على الرغم من هذا كان رأي الدول المجيبة عن الاستبيان أنها "بشكل عام لا تشرك محاكم متخصصة على أساس الموضوع محل النقاش على الرغم أن بعض القضاة على مستويات مختلفة يتخصصون في القضايا الجنائية من قبل الممارسة، وربما يسند إليهم رئيس المحكمة القضايا الجنائية.[1]

تخصص الموظفين

وعلى غرار هذا، حيث أظهرت الهياكل القضائية تخصصات تنظيمية للجريمة السيبرانية أقل منه بالنسبة لإنفاذ القانون فقد سجلت البلدان مستويات من القدرات الفنية بين المدعين المتخصصين أقل من مسئولي إنفاذ القانون. ويعرض الشكل 6-10 ردود البلدان فيما يخص إنفاذ القانون ومهارات تكنولوجيا المعلومات القضائية.[2] بينما سجل عدد قليل للغاية من المدعين العامين للجرائم السيبرانية مهارات متقدمة في تكنولوجيا المعلومات مقارنة بمسئولي إنفاذ القانون المتخصصين في الجريمة السيبرانية، وقد يعكس هذا على نحو جزئي الأدوار الوظيفية المختلفة لكل منهما. على الرغم من أن المشاركة القضائية في التحقيقات تختلف عبر الأنظمة القضائية، وبوجه عام، ربما يُطلب من مسئولي إنفاذ القانون إجراء تحقيقات مبدئية قائمة على الأدلة الجنائية وجمع الأدلة الإلكترونية.

الشكل 6-10: القدرات الفنية للشرطة والمدعين العامين

المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 116 و160. (رقم=54، 29)

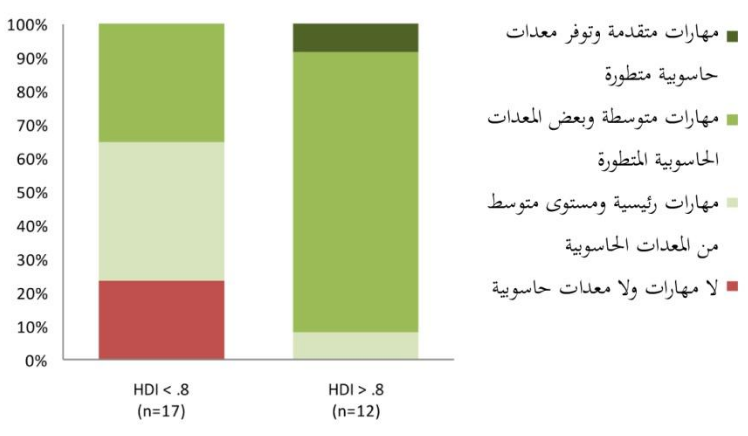
---

[1] استبيان دراسة الجريمة السيبرانية، السؤال 187.

[2] استبيان دراسة الجريمة السيبرانية، السؤال 116 والسؤال 160.

وتتنوع القدرات الفنية للمدعين العامين بدرجة كبيرة وفقا لمستوى تنمية البلد. حيث أفادت البلدان الأكثر تقدما أن حوالي 80 في المائة من المدعين العامين كانت لديهم مهارات متوسطة من تكنولوجيا المعلومات وكانت لديهم وسيلة للتعامل مع الأجهزة المتطورة. و8 في المائة كانوا يتمتعون بمستوى متقدم في مهارات تكنولوجيا المعلومات. ولم تفد أي بلد من البلدان المتطورة عدم امتلاك المدعين العامين مهارات تكنولوجيا المعلومات أو أجهزة الحاسوب.

الشكل 6–11: القدرات الفنية للمدعين العامين



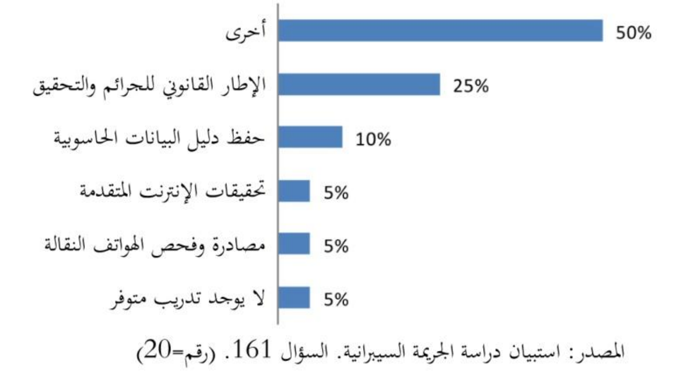
المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 160. (رقم=29)

وفي المقابل، أفاد عدد أكثر من في المائة من البلدان الأقل تقدما أن المدعين العامين المتخصصين إما يتمتعون بالمهارات الأساسية لتكنولوجيا المعلومات ومهارات متوسطة لأجهزة الحاسوب أو لا يتمتعون بشيء على الإطلاق. وتشير تلك النتائج إلى وجود فجوة كبيرة في القدرات. في أحد البلدان الأقل تقدما يتم توفير المعدات الحاسوبية الضرورية *"عند الطلب،"* [1] على الرغم من أن جميع البلدان تقريبا أفادت بأنها تواجه تحديات في كل من التدريب والأجهزة. *"التدريب الفني غير كافٍ"* وتوجد حاجة إلى المزيد من الدعم في مجال التدريب لتحسين النتائج.[2] وأفادت إحدى البلدان الأكثر تطورا أن *"المدعين العامين يتمتعون بمهارات متنوعة من مهارات تكنولوجيا المعلومات المتقدمة والمتوسطة ولكن ليس لديهم القدرة على التعامل مع أجهزة الحاسوب المتطورة أو حتى ذات المستوى المتوسط."* [3]

تطوير الموظفين

تناول التدريب المقدم للمدعين العامين مجموعة من الموضوعات، وأشارت نصف البلدان المجيبة أن المدعين العامين تلقوا


الشكل 6–12: التدريب محل النقاش للمدعين العامين



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 161. (رقم=20)

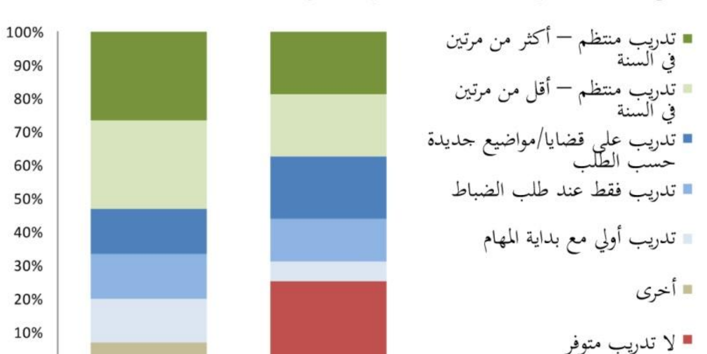
---

[1] استبيان دراسة الجريمة السيبرانية، السؤال 160.
[2] المرجع نفسه
[3] المرجع نفسه

تدريبا في مواضيع متعددة. بالإضافة إلى الموضوعات المحددة في الشكل 6–12 توجد موضوعات أخرى وهي *"تشغيل الإنترنت وأنواع الجريمة السيبرانية بالإضافة إلى التحقيقات والتشريعات*[1] *وأمن المعلومات والحفاظ على الأدلة الإلكترونية المتصلة بجرائم غسيل الأموال."* وأشارت إحدى البلدان "أنه من حين لآخر، يشارك المدعون العامون في التدريب الذي توفره منظمات الشرطة لخبرائها الخاصين بها.[2] موضوع تدريب المدعين العامين المتخصصين ليس متنوعا مثل ذلك الذي لوحظ فيما يتعلق بمسئولي إنفاذ القانون وربما يرتبط هذا مع الاختلافات المتجسدة في أدوار كل منهم داخل عملية العدل الجنائي. وأكدت العديد من البلدان النامية حاجتها للمزيد من التدريب الفني للمدعين العامين. وأشارت إحدى البلدان، على سبيل المثال: *"إن الإعداد في القانون الجنائي ذو جودة عالية والتدريب الفني غير كافي."*[3] وأشارت أخرى "أنهم في حاجة إلى المزيد من الدعم في مجال التدريب لتحسين النتائج.[4] وأكد آخرون أنهم في حاجة إلى المزيد من التدريب في تكنولوجيا المعلومات.[5]

وأظهرت البلدان المجيبة عن الاستبيان أيضا تباينا كبيرا في تكرار ومدة التدريب للمدعين العامين المتخصصين. وبوجه عام، أفاد أكثر من 40 في المائة من البلدان المجيبة أن المدعين العامين قد تلقوا تدريبا منتظما وأن 20 في المائة تلقوا تدريبا أكثر من مرتين في العام. وكما هو الحال في التخصص التنظيمي والقدرات الفنية فإن الاختلافات أيضا واضحة حسب مستوى تنمية البلد.

الشكل 6–13: تكرار التدريب للمدعين العامين

المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 162. (رقم=31)

ربع المدعين العامين المتخصصين في البلدان الأقل تطورا ليس لديهم تدريب متخصص. ويتلقى حوالي 40 في المائة تدريبا منتظما.

وعلى النقيض، لم تذكر أي من البلدان في أكثر الطوائف المتقدمة بعدم توفر التدريب وأفاد أكثر من نصف تلك البلدان أن المدعين العامين المتخصصين قد تلقوا تدريبا منتظما لأكثر من مرة في العام. وقد أوردت العديد من البلدان المتطورة بالتفصيل الجوانب الإضافية المتعلقة بمعدل تكرار التدريب والذي يتضمن "برامج

[1] استبيان دراسة الجريمة السيبرانية، السؤال 161.
[2] المرجع نفسه
[3] استبيان دراسة الجريمة السيبرانية، السؤال 160.
[4] المرجع نفسه
[5] المرجع نفسه

تدريبية متعددة التخصصات سنويا" "ووحدات التعلم الإلكتروني" "وحضور المؤتمرات" "وتدريب شهري حول الموضوعات المتخصصة التي يجريها خبراء داخليون وخارجيون".[1]

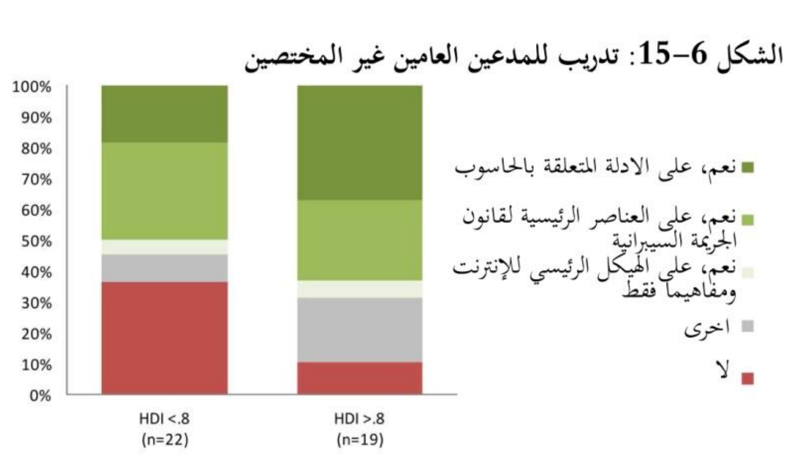

الشكل 6–14: مقدّم التدريب للمدعين العامين المختصين



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 163. (رقم=34)

أكثر مقدمي التدريب شيوعا للمدعين العامين المتخصصين كانت وحدة وكالة القضاء. قد أنشأت الأكاديميات القضائية ووزارات العدل بالإضافة إلى الوكالات المتعددة حوالي 10 في المائة من مقدمي التدريب للمدعين العامين. وقد ذُكر أن نسبة صغيرة للغاية – 3 في المائة– من المدعين العامين المتخصصين قد تدربوا على أيدي منظمات إقليمية ودولية. وقد ذكرت 6 في المائة من البلدان أنه لم يتم إجراء أي تدريب متخصص للمسئولين القضائيين.

وقد أقر عدد من البلدان المجيبة عن الاستبيان بأهمية توفير تدريب بشأن الجريمة السيبرانية للمدعين العامين غير المتخصصين. فعلى سبيل المثال أفادت إحدى البلدان بأنها "طورت خلال الأعوام الماضية العديد من الأنشطة من أجل تيسير المعرفة الكافية بتلك الجريمة السيبرانية لكافة المدعين العامين بهدف تزويدهم بأفضل المهارات المتعلقة بالتكنولوجيا الحديثة.[2] وأكدت إحدى البلدان أن التدريب الواسع "لم يكن يهدف فقط إلى إثراء معرفة المبدأ القانوني لهذه الجرائم ولكن يسعى أيضا إلى زيادة الوعي حول أهمية تبني


الشكل 6–15: تدريب للمدعين العامين غير المختصين

المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 164. (رقم=41)

---

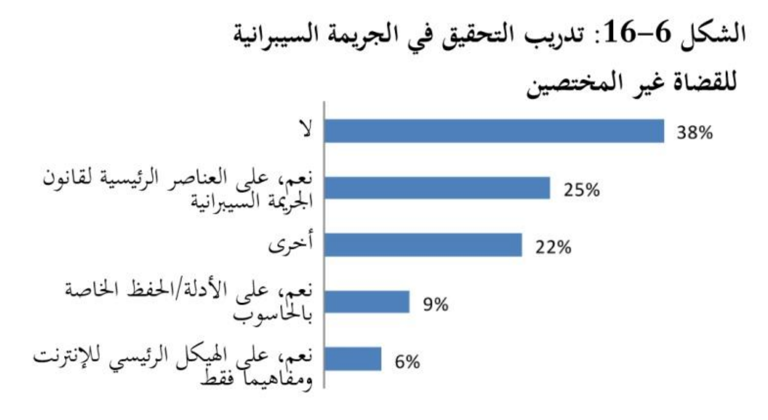
[1] استبيان دراسة الجريمة السيبرانية، السؤال 162.

[2] استبيان دراسة الجريمة السيبرانية، السؤال 164.

المفاهيم الإجرائية الكلاسيكية في أنماط التكنولوجيا الحديثة وإمكانيات الأدلة الجنائية.[1] وبوجه عام، أفادت حوالي 60 في المائة من البلدان بوجود تدريب خاص بالجريمة السيبرانية للمدعين العامين غير المتخصصين. ويوضح الشكل 6-15 الاختلافات وفقا لمستوى تنمية البلد؛ حيث أن حوالي 40 في المائة من البلدان الأقل تطورا قد أفادت أن المدعين العامين غير المتخصصين لا يتلقون أي شكل من أشكال التدريب بخصوص الجريمة السيبرانية.

من بين الأجهزة القضائية، أفاد حوالي 40 في المائة من البلدان المجيبة عن الاستبيان بعدم وجود تدريب متخصص للقضاة في الجريمة السيبرانية. وأفاد الربع بوجود تدريب على العناصر الأساسية لقانون الجريمة السيبرانية.

الشكل 6-16: تدريب التحقيق في الجريمة السيبرانية للقضاة غير المختصين



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 192. (رقم=32)

وكانت ردود العديد من البلدان المجيبة عن الاستبيان مشابهة لردود بلدان شمال أوروبا التي ذكرت تعليق "بأنه لا يوجد قضاة متخصصين، ويغطي التدريب البرامج التدريبية المستمرة التي ينظمها القضاء وهو مفتوح لجميع القضاة. وينظم سنويا وغالبا ما يستمر لمدة يومين، ويعتبر هذا التدريب بالأحرى ذو طبيعة عامة باعتباره مقدمة للجرائم السيبرانية.[2] وأفادت إحدى البلدان بوجود تدريب قضائي "يهدف إلى تناول الحالات بشأن التشريعات الوطنية في الجريمة السيبرانية، إضافة إلى ملخصات القضايا الحديثة.[3] وبوجه عام، أكدت البلدان بوجود حاجة ملحة للتدريب القضائي على قانون الجريمة السيبرانية، وجمع الأدلة، والمعرفة الأساسية والمتقدمة في الحاسوب.[4]

وأفيد بأن ذلك التدريب الذي يحدث حاليا تجريه مجالس ومراكز التدريب القضائية، ووحدات التدريب القضائية والمحاكم، والوزارات أو معاهد القضاء. وأفادت العديد من البلدان أن القضاة ربما *"يختارون طواعية المشاركة في برامج التطوير المهني، وتتنوع البرامج في المحتويات التي تتناولها ولا توجد مواد تدريب محددة للقضاة المشاركين في قضايا الجريمة السيبرانية"*.[5]

---

[1] المرجع نفسه

[2] استبيان دراسة الجريمة السيبرانية، السؤال 164.

[3] المرجع نفسه

[4] المرجع نفسه

[5] استبيان دراسة الجرائم السيبرانية، السؤال 192.

5-6 بناء القدرات والمساعدة الفنية

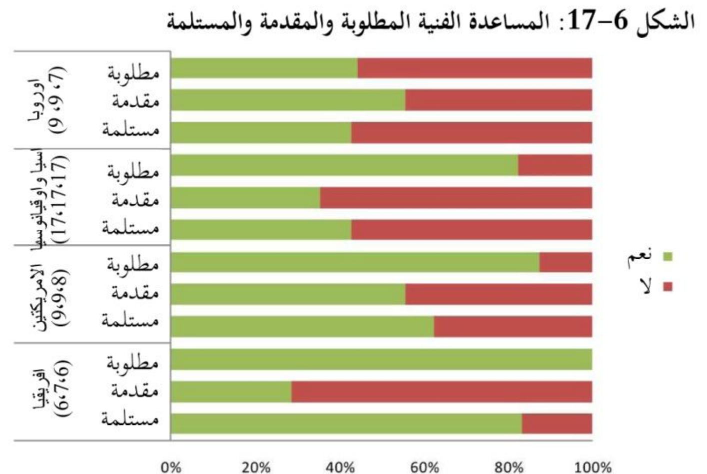
الاستنتاجات الرئيسية:

- أفاد 75 في المائة من البلدان المجيبة في جميع مناطق العالم بحاجتها إلى مساعدة فنية في مجال الجريمة السيبرانية
- وتم تقديم المساعدة الفنية للبيانات في الغالب في مجال تحقيقات الجريمة السيبرانية العامة والتحقيق الجنائي الحاسوبي. وتشير تلك الحاجة إلى وجود إمكانية للمساعدة في مجالات التعاون الدولي والتقاضي ودعم المحاكمات على وجه الخصوص
- مجموعة من تقارير المؤسسات الحكومية التي تطلب مساعدة فنية، الأمر الذي يؤكد الحاجة لأسلوب شامل ومتعدد التخصصات للمساعدة الفنية الخاصة بالجريمة السيبرانية
- تشير سيطرة أنشطة المساعدة الفنية التي تستمر لأقل من شهر واحد إلى الحاجة الشديدة لاستمرارها لمدة أطول فضلا عن وجود استثمارات مستدامة

وكرد على الأسئلة الخاصة بقدرة إنفاذ القانون، تقوم سلطات النيابة العامة والمحكمة بمنع الجريمة السيبرانية ومكافحتها. وقد شمل استبيان الدراسة أسئلة حول احتياجات البلدان للمساعدة الفنية وتقديمها لها.

وبشكل عام أفادت 75 في المائة من البلدان المجيبة في جميع مناطق العالم بحاجتها إلى مساعدة فنية في بعض المجالات الموضوعية المرتبطة بالجريمة السيبرانية حيث أشارت كل بلد مجيبة في أفريقيا إلى حاجتها إلى مساعدة فنية.

الشكل 6–17: المساعدة الفنية المطلوبة والمقدمة والمستلمة



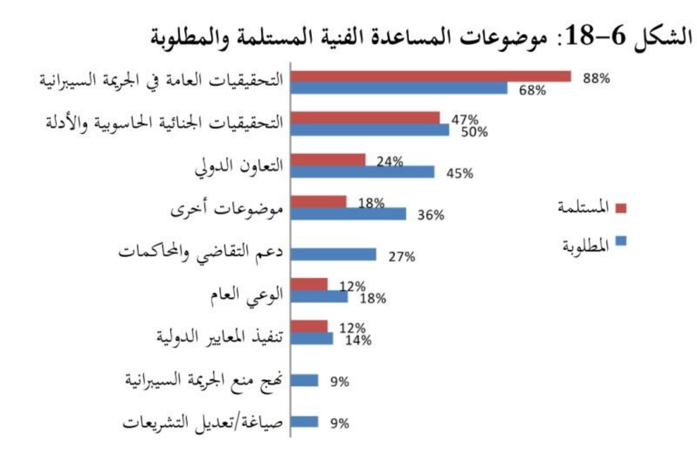
المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 241، 253، 250. رقم=40، 42، 39)

أفاد أكثر من 70 في المائة من جميع البلدان المجيبة بتقديمها بعض أشكال المساعدة الفنية لبلدان أخرى على الرغم من إفادة أقل من 20 في المائة من البلدان بحصولها على مساعدة فنية. وقد يشير هذا إما إلى تركيز عدد كبير من البلدان المانحة على عدد أقل من البلدان المتلقية وإما إلى عدم تجاوب نسبة كبيرة من البلدان الأقل نموا مع استبيان الدراسة.

وبالنسبة للبلدان الأوروبية، أفاد أكثر من نصف تلك البلدان بحصولها على مساعدة فنية في حين أفاد أقل من نصفها بحاجتها أو تقديمها مساعدة فنية في مجال الجريمة السيبرانية. ففي آسيا، وأوقيانوسيا والأمريكتين، أفاد أكثر من 80 في المائة من البلدان بحاجتها إلى المساعدة الفنية. وأفادت غالبية البلدان في أسيا وأوقيانوسيا بتقديمها مساعدة فنية، وحصول أقل من نصف البلدان على مساعدة فنية. وفي الأمريكتين، قدّم أقل من نصف البلدان مساعدة فنية في حين تلقى أكثر من ثلث البلدان بعض أشكال المساعدة الفنية.

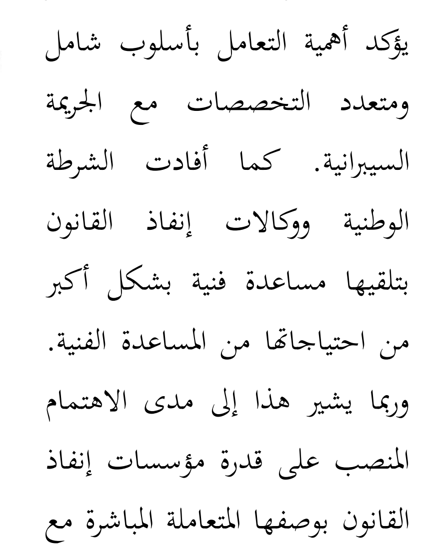
الموضوعات– كانت "التحقيقات العامة في الجريمة السيبرانية" مجال الاختصاص الأكثر ذكرا وشيوعا لكل من المساعدة الفنية المتلقاة والمطلوبة، ومجال الاختصاص الوحيد الذي تم من أجله الإبلاغ عن مساعدة فنية متلقاه تتجاوز اللازم منها. ويمكن أن يشير هذا إلى وجود إمكانية في أن تتجاوز المساعدة الفنية الخاصة بالجريمة السيبرانية الاهتمام التقليدي حول تحقيقات نفاذ القانون فضلا عن شمولها مجموعة أكبر من المجالات. وبشكل خاص، تمثل مجالات "التعاون الدولي" و "التقاضي ودعم المحاكمات" ساحات يتم الإبلاغ فيها عن المساعدة المطلوبة، لكن تم الإبلاغ فيها عن القليل الذي تم تقديمه. وأفادت إحدى هيئات الأمم المتحدة أن "الحكومات تطلب المزيد من التدريب في تلك المجالات".[1]

الشكل 6–18: موضوعات المساعدة الفنية المستلمة والمطلوبة



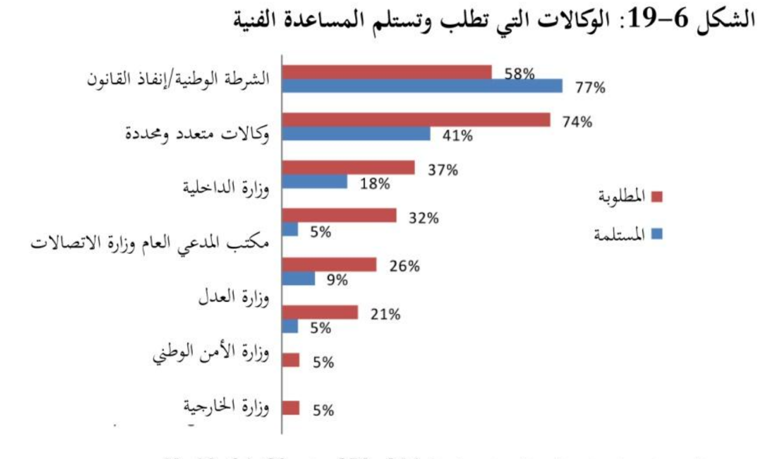
المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 243 و251. (رقم=17، 36، 22، 61)

المؤسسات – أفادت مجموعة كبيرة من الجهات الحكومية بحاجتها وتلقيها مساعدة فنية– الأمر الذي



يؤكد أهمية التعامل بأسلوب شامل ومتعدد التخصصات مع الجريمة السيبرانية. كما أفادت الشرطة الوطنية ووكالات إنفاذ القانون بتلقيها مساعدة فنية بشكل أكبر من احتياجاتها من المساعدة الفنية. وربما يشير هذا إلى مدى الاهتمام المنصب على قدرة مؤسسات إنفاذ القانون بوصفها المتعاملة المباشرة مع

الشكل 6–19: الوكالات التي تطلب وتستلم المساعدة الفنية



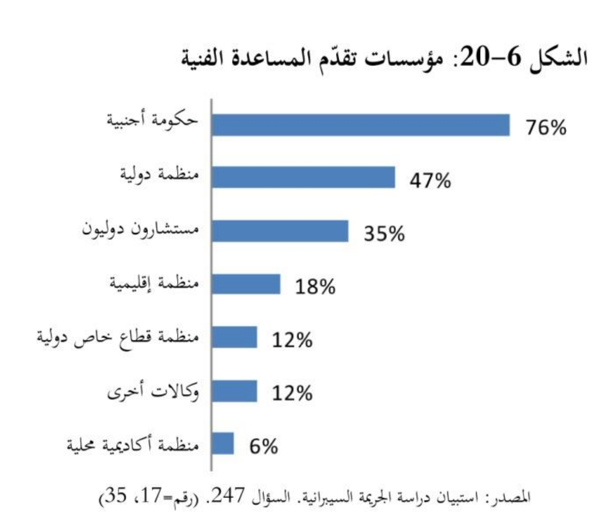
المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 244 و252. (رقم=22، 34، 19، 49)

[1] استبيان دراسة الجريمة السيبرانية (المنظمات الحكومية الدولية والأوساط الأكاديمية). السؤال رقم 20.

الجريمة السيبرانية. وربما يتوافق مستوى أعلى من تقديم المساعدة الفنية المبلغ عنها والمتعلقة بوكالات إنفاذ القانون مع مستويات أعلى مبلغ عنها من التخصص التنظيمي والوظيفي بين وكالات إنفاذ القانون من تلك الخاصة بأجهزة العدالة الجنائية (إنفاذ القانون والتحقيقات). ويبين الشكل 6-19 أيضا الدرجة المحدودة نسبيا التي تلقت عندها مؤسسات مثل النيابة والمحاكم المساعدة الفنية، الأمر الذي يؤكد الصورة الموضوعية في الشكل 6-18.

التسليم (للمساعدة الفنية) والجهات المانحة– تعتبر الحكومات المؤسسات الأكثر تقديما للمساعدة الفنية (أكثر من 75 في المائة) تليها المنظمات الدولية والاستشاريين الدوليين. وتعتبر المنظمات الإقليمية مثل الاتحاد الأفريقي، ومنظمة الدول الأمريكية ومجلس أوروبا باعتبارها من مانحي المساعدة الفنية بنسبة 20 في المائة من الدول المجيبة. وتجدر الإشارة إلى أنه من الممكن أن تستخدم هيئات "المنح" الخاصة بالمساعدة الفنية أساليب متعددة. ومن الممكن القيام "بمنح" مشروع أو برنامج مساعدة فنية معينة من خلال الشراكة بين الحكومات وبين المنظمات الدولية والإقليمية، وبين الاستشاريين المستقلين والمؤسسات الأكاديمية. ومن الجدير بالذكر أن مؤسسات القطاع الخاص الدولية، التي غالبا ما تقوم معها مثل تلك الشراكات، قد منحت مساعدة فنية لحوالي 10 في المائة من الدول المجيبة، الأمر الذي يؤكد أهمية مؤسسات القطاع الخاص بوصفها من الشركاء الرئيسيين في هذا المجال.

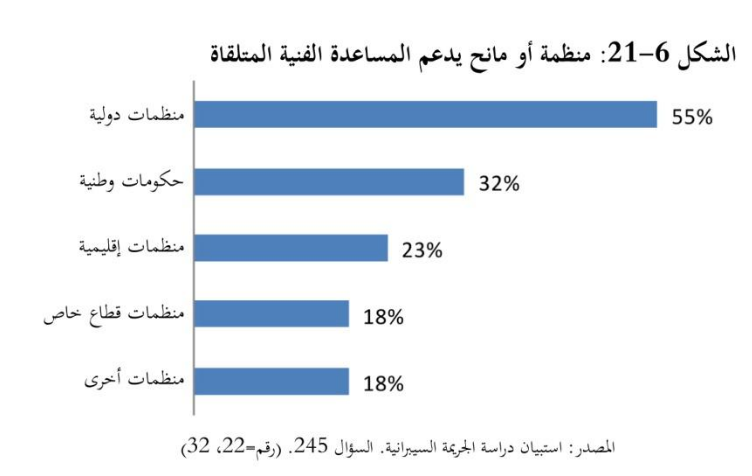
الشكل 6-20: مؤسسات تقدّم المساعدة الفنية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 247. (رقم=17، 35)

وقد أكدت إجابات المنظمات الحكومية الدولية على استبيان الدراسة الدور الذي تؤديه تلك المنظمات في تقديم المساعدة الفنية حيث تقدم المنظمات المساعدات الفنية لمجموعة متنوعة من الموضوعات بدءا من أساليب التحقيق العامة، وحفظ التحقيقات الجنائية والأدلة إلى تطوير التشريعات والتعاون بين القطاعين العام والخاص، ووضع المعايير الدولية فضلا عن التوعية. وقد أكد عدد من هيئات الأمم المتحدة على أهمية تحقيق *أسلوب شامل ومتعدد*

الشكل 6-21: منظمة أو مانح يدعم المساعدة الفنية المتلقاة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 245. (رقم=22، 32)

المستويات" للمساعدة الفنية.[1] وقد أكد الكثيرون أنه من المهم بناء قدرات في مجالات الشراكة مثل "*شبكات مؤسسات التدريب القضائي*" فضلا عن استخدام أسلوب مثل "تدريب المدربين لكي يكونوا محققين/ مفتشين في مجال جريمة تكنولوجيا المعلومات".[2] ذكرت إحدى المنظمات على سبيل المثال أنه من المهم أن تستخدم "*جميع المعلومات والمواد*" من خلال "*مشاركين يقدمون نفس التدريب في بلدانهم بصورة محلية*".[3] وبناء على الاهتمام بالبرنامج، تغير الجمهور المستهدف من كونه شخصيا مثل ضباط إنفاذ القانون والمحققين الجنائيين، إلى كونه مؤسسيا كوزراء الداخلية والعدل والاتصالات. وقد قدمت المنظمات الدولية تدريبا في كل منطقة؛ وأفادت تقارير كثيرة بأن برامج التدريب مستمرة وتحظى بطلب كبير، على الرغم من أنها أحيانا ما يحدها توافر الموارد.

وقد طرح عدد من المنظمات الحكومية الدولية سؤالا مهما خاصا *بالمعايير والتوثيق*. وقد أشارت إحدى المنظمات إلى استخدام التدريب الجنائي "*المعتمد بمعرفة جامعة ... ويتم إلقائه على 3 أقسام؛ دورة المستوى التأسيسي في عام 2010، ودورات متقدمة في عام 2011، ودرجة ماجستير على الإنترنت مؤجلة حتى عام 2012*"[4]. وأكدت إحدى هيئات الأمم المتحدة على التحدي الخاص بتحديد ومعرفة المعايير المهنية التي يتعين إتباعها فضلا عن تشجيعها أثناء إلقاء التدريب. وعلى سبيل المثال، أفادت نفس الهيئة أنه "*لا وجود لأي إجماع حول متطلبات المنهج [الجنائي]. ومع تطور المجال، فمن المحتمل أن يكون ثمة عروض لدورات فضلا عن التوحيد القياسي*"[5] في حين أكدت هيئات أخرى تابعة للأمم المتحدة تحدي نقص الموارد فضلا عن الوعي بخصوص مشكلة الجريمة السيبرانية نظرا لمنع تقديم المساعدة الفنية. وأشارت إحدى هيئات الأمم المتحدة إلى أنه "نتمتع بالخبرة إلا أننا لا نملك الموارد اللازمة لمكافحة الجريمة السيبرانية".[6]

ويأتي الدعم الخاص بالمساعدة الفنية من عدد صغير نسبيا من الحكومات الوطنية والمنظمات الدولية والإقليمية فضلا عن مؤسسات القطاع الخاص. وتعد المنظمات الدولية أكبر مصدر دعم خاص بالمساعدة الفنية مع إشارة أغلبية البلدان (55 في المائة) إلى بعض أشكال المساعدة الفنية من هذا المصدر. كما أشارت إحدى هيئات الأمم المتحدة إلى أهمية "*التدريب الذي يتم تقديمه بمعرفة المنظمات ذات الخبرة في المنطقة*"[7]. وأشار ثلث المجيبين تقريبا إلى الحكومات الوطنية باعتبارها جهات مانحة داعمة في حين تفسر المنظمات الإقليمية ربع الدعم بالمساعدة الفنية. وأشار 20 في المائة من المجيبين تقريبا إلى القطاع الخاص وأنواع المنظمات الأخرى باعتبارها جهات مانحة ورعاة للمساعدة الفنية.

---

[1] المرجع نفسه.

[2] المرجع نفسه.

[3] المرجع نفسه.

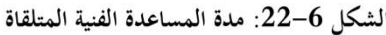
[4] المرجع نفسه.

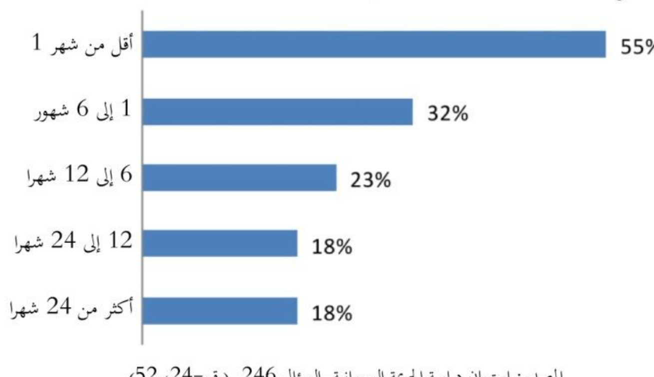
[5] استبيان دراسة الجريمة السيبرانية (المنظمات الحكومية الدولية والأوساط الأكاديمية). السؤال رقم 51.

[6] المرجع نفسه.

[7] استبيان دراسة الجريمة السيبرانية (المنظمات الحكومية الدولية والأوساط الأكاديمية). السؤال رقم 51.

المدّة – أشارت تقارير إلى استمرار 60 في المائة تقريبا من برامج المساعدة الفنية لمدة أقل من شهر واحد. وقد استمر ربع تلك البرامج لمدة تزيد عن عامين. وعلى الرغم من أنه من الممكن أن تكون احتياجات المساعدة الفنية المتعلقة بالجريمة السيبرانية طويلة المدى، ومتوسطة المدى، وقصيرة المدى، إلا أن سيطرة أنشطة المساعدة الفنية قصيرة المدى تشير إلى الحاجة لمدى أطول، واستثمار مستدام ينصب على بناء القدرة الهيكلية الرئيسية الخاصة بنطاق السلطات الحكومية وأصحاب المصلحة المشتركين في مواجهة الجريمة السيبرانية.


الشكل 6–22: مدة المساعدة الفنية المتلقاة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 246. (رقم=24، 52)

الفصل السابع: التعاون الدولي

يتناول هذا الفصل التعاون الدولي الرسمي وغير الرسمي استجابة لتحدي الجريمة السيبرانية عبر الوطنية. ويتوصل إلى أن الاعتماد على الآليات التقليدية على نطاق واسع، مثل المساعدة القانونية المتبادلة، وظهور تكتلات التعاون بين البلدان، ونقص الوضوح بشأن إمكانية وصول سلطات إنفاذ القانون إلى البيانات خارج حدود الولاية القضائية تمثل كلها تحديات أمام استجابة عالمية فاعلة.

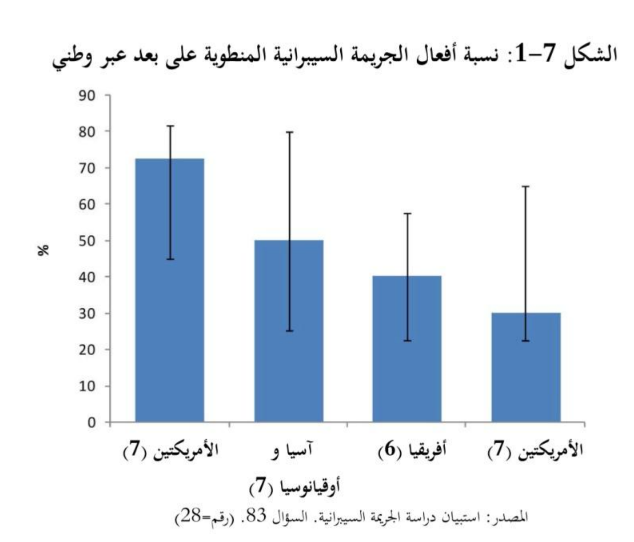
7-1 السيادة، والولاية القضائية، والتعاون الدولي

الاستنتاجات الرئيسية

- يظهر "البعد عبر الوطني" للجرائم السيبرانية عندما يمتد أي عنصر من الجرم، أو الأثر الفعلي لهذا الجرم إلى أي إقليم آخر، أو عندما يمتد أي جزء من *طريقة ارتكاب* الجرم إلى أي إقليم آخر
- أفادت البلدان المجيبة على الاستبيان بخصوص الدراسة أن المعدلات الإقليمية للأفعال المنطوية على جريمة سيبرانية والتي تتضمن بعدا عبر وطني تتراوح ما بين 30 و70 في المائة
- وهذا يشمل قضايا السيادة والولاية القضائية والتحقيقات عبر الوطنية والأدلة خارج حدود الولاية القضائية وأي من متطلبات التعاون الدولي

الجريمة السيبرانية باعتبارها جريمة عبر وطنية

الشكل 7-1: نسبة أفعال الجريمة السيبرانية المنطوية على بعد عبر وطني



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 83. (رقم=28)

لا تعد الجريمة السيبرانية بأي حال من الأحوال أول صورة "جديدة" للجريمة تتطلب استجابة عالمية. فعلى مدار العقود السابقة تطلبت الإجراءات العالمية التعامل مع تحديات مثل الاتجار غير المشروع بالمخدرات والجريمة المنظمة عبر الوطنية، ويشمل ذلك العمل من خلال تطوير اتفاقيات دولية. ورغم ذلك، أصبح من البديهي أن الجريمة السيبرانية تمثل تحديات بالنسبة للتعاون الدولي. واثناء جمع المعلومات من أجل الدراسة، أفادت

أكثر من نصف البلدان أن ما بين 50 إلى 100 في المائة من الأفعال التي تنطوي على جريمة سيبرانية التي تعاملت معها الشرطة تضمنت "*عنصرا عبر وطني*".[1] ويظهر الشكل أن بلدان أوروبا ينظر إليها باعتبارها صاحبة أكبر نسبة من الأفعال التي تنطوي على جريمة سيبرانية التي تنطوي على بعد عبر وطني. بينما ينظر إلى أفريقيا والأمريكتين باعتبارهما صاحبتا أقل نسبة.[2]

وقد أفادت إحدى بلدان أوروبا الشرقية أن "*حوالي 80 في المائة من الأفعال التي تنطوي على جريمة سيبرانية خاضعة للتفتيش [من قبل سلطات إنفاذ القانون المحلية] تتعلق بأكثر من بلد*".[3] بينما أشار بلد آخر من غرب أفريقيا أن معظم المجني عليهم المستهدفين من طرف مرتكبي الجريمة السيبرانية داخل منطقتهم يقعون "*خارج الحدود الوطنية*".[4] كما أشارت بلدان أخرى أن معظم المخالفات التي يجري الإبلاغ عنها "*قد ارتكبت خارج*" منطقتها. بينما لاحظ آخرون أن "*في معظم الحالات نتصرف باعتبارنا وسيط*".[5] وقد أشارت البلدان أن استخدام الخوادم الوكيلة والأثر المتنامي لمواقع التواصل الاجتماعي كانت من بين العوامل التي أدت إلى زيادة عدد الحالات التي تتضمن بعدا عبر وطني.[6] وقد أفادت إحدى البلدان أن مرتكبي الانتهاكات على دراية تامة بقضايا الولاية القضائية ويستخدمون عن عمد مصادر الإنترنت، مثل خوادم البريد، التي تقع في الخارج في محاولة لإخفاء أي أدلة لأنشطتهم غير القانونية[7]. وتعد وجهة النظر غير موحدة على أي حال. فقد أفادت إحدى بلدان أمريكا الجنوبية أن عددا لا بأس به من القضايا عبر الوطنية كانت "محلية الأصل".[8]

ويدرس هذا الفصل سبل التعاون ما بين الولايات القضائية والتعاون الدولي لمكافحة الجريمة السيبرانية — على مستوى صكوك الجريمة السيبرانية الدولية والإقليمية إضافة إلى قوانين الدول وممارساتها. وهو يضع المعلومات المجمعة من الاستبيان الخاص بالدراسة في الإطار القانوني الدولي للسيادة والولاية القضائية والتعاون الدولي في المسائل الجنائية.

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 83. بعض الدول التي لم تتمكن من تقديم أرقام دقيقة حسبت النسبة على أنها "مرتفعة جدا".

[2] يوضح الشكل القيم المتوسطة باستخدام الربعين الأعلى والأقل ممثلة بأشرطة الخطأ.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 83.

[4] المرجع نفسه

[5] المرجع نفسه

[6] المرجع نفسه

[7] المرجع نفسه

[8] المرجع نفسه

نقطة البداية – السيادة والولاية القضائية

تتمثل نقطة البداية للولاية القضائية للدولة والتعاون الدولي في السيادة. وتخضع المساواة في سيادة الدول للحماية بموجب قواعد القانون الدولي العام العرفي. ويشمل هذا التزام الدول بعدم "*التدخل بأي صورة أو لأي سبب كان في الشؤون الداخلية والخارجية للدول الأخرى*".[1]

تقع مسائل إنفاذ القانون والعدالة الجنائية ضمن النطاق الحصري للدولة ذات السيادة – ونتيجة لذلك، على نحو تقليدي، ارتبطت *الولاية القضائية* الجنائية بالإقليم الجغرافي. لذا يجب على الدول الامتناع عن ممارسة الضغط لتحمل الدول الأخرى بشأن سلوك بعض الهيئات الوطنية، مثل وكالات إنفاذ القانون أو القضاء.[2] لا يجوز إلقاء القبض على الأشخاص، ولا يجوز إرسال أي استدعاء، ولا يجوز إجراء تحقيقات الشرطة أو الضرائب في إقليم أي دولة أخرى، إلا بموجب شروط معاهدة محددة أو أي موافقة أخرى.[3]

بالطبع، لا تحدث جميع الجرائم ببساطة داخل الولاية القضائية للمنطقة. وإذا كان هذا هو الحال، فقد جاء القانون الدولي ليعترف بعدد من الأساسات للولاية القضائية *خارج الإقليم* في المسائل الجنائية.[4] وتلخص الأسس المشتركة بين القانون الوطني والاتفاقيات الدولية في الجدول أدناه. والعامل المشترك بين جميع هذه المبادئ هو المعنى الواسع لشرط وجود "صلة كافية" أو "رابط حقيقي" بين الجرم والولاية القضائية اللازمة التي تمارسها الدولة.[5]

---

[1] على هذا النحو، لدى الدول الحق في السيادة وسلامة أراضيها وحرية تقرير نظامها السياسي والاقتصادي والاجتماعي، بما في ذلك جميع المسائل التي تقع داخل نطاق ولايتها القضائية المحلية. أنظر الإعلان بشأن عدم جواز التدخل بجميع أنواعه في الشؤون الداخلية للدول، ملحق قرار الأمانة العامة A/RES/20/2131 (20) المؤرخ 21 كانون الأول/ديسمبر 1965. يرجى أيضا الرجوع إلى قضية *قناة كورفو*، تقارير محكمة العدل الدولية لسنة 1949، 35، قضية الأنشطة العسكرية وشبه العسكرية، تقارير محكمة العدل الدولية لسنة 1986، 202، وقضية نيكاراغوا، تقارير محكمة العدل الدولية لسنة 1986، 14، 10-109.

[2] حتى، على سبيل المثال، عندما يخضع مواطنو إحدى الدول للمحاكمة في الخارج، يكون المبدأ الأساسي هو أن الدولة لا يمكنها التدخل في الإجراءات القضائية لأي دولة ذات سيادة نيابة عن مواطنيها. وعلى غرار ذلك، لا يمكن للدول اتخاذ أي تدابير في إقليم أي دولة أخرى عن طريق إنفاذ القوانين السارية على موطنيها دون موافقة الأخيرة. أنظر Cassese, A.,International Law، صفحة 53.

[3] Brownlie, I., 2003. *Principles of Public International Law*. 6th ed. Oxford: Oxford University Press. صفحة 306.

[4] Jeschek, H. H., Weigend, T., 1996. *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5th edn. Berlin: Duncker & Humbold. صفحة 167 وما يليها.

[5] Epping, V. and Gloria, C., 2004. Der Staat im Völkerrecht. *In*: Ipsen, K., (ed.) *Völkerrecht*. 5th ed. Munich: C.H. Beck. صفحة 321-22.

مبادئ الولاية القضائية الجنائية	
مبدأ الإقليمية	يمكن لأي دولة محاكمة الأنشطة التي تحدث في إقليمها، حتى إذا كان مرتكب الجرم أجنبيا.
(مبدأ الإقليمية الموضوعية)	إذا كان مرتكب الانتهاك خارج الإقليم، يشمل الاختصاص الإقليمي الموضوعي برغم ذلك متى كان أحد العوامل المكونة للجريمة، وخاصة الآثار المترتبة عليها، التي حدثت داخل الإقليم. يضمن مبدأ الإقليمية أن الدولة التي بدأ الفعل فيها، والدولة التي ارتكب فيها الجرم يمكنها محاكمة مرتكب الانتهاك المزعوم[1]
مبدأ الآثار الجوهرية	تنشأ الولاية القضائية على التصرف الأجنبي الذي تنشأ عنه آثار جوهرية داخل الإقليم[2]
مبدأ الجنسية	تنشأ الولاية القضائية بناء على جنسية الأفراد المعنيين[3]
(الإيجابي)	تنشأ الولاية القضائية بناء على جنسية مرتكب الجرم، أينما ارتكبت الجريمة
(السلبي)	تنشأ الولاية القضائية بناء على جنسية المجني عليه، أينما ارتكبت الجريمة
محل الإقامة	تنشأ الولاية القضائية بناء على مكان محل إقامة مرتكب الجريمة[4]
مبدأ الحمائية	تنشأ الولاية القضائية متى كان التصرف الإجرامي يمثل تهديدا لأمن الدولة المعنية أو يمس مصالحها الحيوية.[5]
مبدأ العالمية	تنشأ الولاية القضائية على أي متهم يرتكب عددا صغيرا من "الجرائم الدولية"، مثل القرصنة وجرائم الحرب، والمخالفات الجسيمة لمعاهدات جينيف، بصرف النظر عن الإقليم أو جنسية الأفراد المتورطين.[6] ويقتصر المبدأ عادة على المواقف التي تكون فيها الدولة ذات الولاية القضائية غير قادرة أو ليست على استعداد للمحاكمة

من المهم ملاحظة أن استخدام هذه الصور من الولاية القضائية للبلدان —سواء بناء على القانون الوطني أو الاتفاقيات الدولية — لا يلغي تلقائيا عملية السيادة وعدم تداخل المبادئ. ولا زال الإجراء المادي للتحقيق الجنائي على أرض أجنبية (في ظل مبدأ المبدأ الوقائي أو مبدأ الجنسية السلبية، على سبيل المثال) موافقة الدولة

[1] *Lotus* case, PCIJ, Series A, No. 10, 1927, 23, 30

[2] أنظر Hayashi, M., 2006. Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace. In Law 6:285

[3] أنظر Shaw, M., 2003. *International Law.* p.579 et seq. and Cassese, A., 2005. *International Law.* صفحة 451 وما يليها.

[4] Jeschek, H. H., Weigend, T., 1996. *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5th edn. Berlin: Duncker & Humbold. صفحة 169.

[5] Simma, B., Mueller, A., 2012. Exercise and the Limits of Jurisdiction. In: Crawford, J. and Koskenniemi, M., (eds.) The Cambridge Companion to International Law، صفحة 134، 143.

[6] Cassese, A., 2005. *International Law*، صفحة 451-452.

الأجنبية.[1] لذا تنتج الولاية القضائية التي تطالب بها الدولة، على نحو منفصل، من السؤال عن عدم التدخل أو مخالفة السيادة.

أنظمة المساعدة القانونية الدولية

ومن أجل إدارة عملية الموافقة على إجراء تحقيقات إنفاذ القانون والعدالة الجنائية خارج إقليم الدولة، يوجد عدد من الترتيبات القانونية وغير الرسمية فيما بين الدول، على مستوى ثنائي أو متعدد الأطراف. وتعد المعاهدات بشأن التسليم الرسمي للمشتبه فيهم من بلد واحد إلى بلد آخر، على سبيل المثال، من بعض الأمثلة القديمة المتعارف عليها في القانون الدولي.[2] وتصاغ معاهدات "التسليم" هذه –إضافة إلى غيرها من صور التعاون الدولي (التي يجري مناقشتها أدناه)– بعناية لضمان احترام آلياتها لمبادئ السيادة الأساسية. وتنص المادة 4 من اتفاقية الجريمة المنظمة، على سبيل المثال، على: *"تؤدي الدول الأطراف التزاماتها بمقتضى هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة والسلامة الإقليمية للدول، ومع مبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى."* وتستمر المعاهدة في توضيح أن: *"ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي."*

إضافة إلى التسليم، تشمل الأدوات الرئيسية للتعاون الدولي تقديم المساعدة في تجميع الأدلة لتستخدم في القضايا الجنائية ("المساعدة القانونية المتبادلة") وترتيبات نقل المحكوم عليهم دوليا.[3] ويمكن تعريف التسليم باعتباره عملية حيث تطلب إحدى الدول إعادة أي متهم بجريمة بالقوة للمثول أمام المحاكم أو قضاء عقوبة في الدولة التي طلبت ذلك.[4] ولا ينص القانون الدولي العرفي على أي "التزام تسليم عام."[5] وتكون الترتيبات عادة بناء على اتفاقيات ثنائية أو متعددة الأطراف في المستقبل في حال طلب ذلك.[6] ولتجنب "فجوات" الولايات القضائية،

---

[1] Brownlie, I., 2003. *Principles of Public International Law*. 6th ed. Oxford: Oxford University Press. صفحة 306. للحصول على مثال وطني قانوني على حظر "الأنشطة غير المشروعة نيابة عن أي دوبة أجنبية" أنظر المادة 271 من القانون الجنائي السويسري: *"كل من يحاول القيام بأنشطة نيابة عن أي دولة أجنبية في الإقليم السويسري دون تفويض مشروع، ومتى كانت تلك الأنشطة على مسؤولية أي سلطة عامة لأي موظف عام، يخضع للسجن."* وللحصول على مثال عملي على أسلوب المحققين الجنائيين الأجانب، أنظر: http://www.rcmp-grc.gc.ca/interpol/fcip-pcece-eng.htm.

[2] Magnuson, W., 2012. The Domestic Politics of International Extradition. *Virginia Journal of International Law*, 52(4):839-891

[3] للحصول على نبذة عامة، أنظر مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012. *دليل المساعدة القانونية المتبادلة وتسليم المجرمين* ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012. *كتيب النقل الدولي للأشخاص المحكوم عليهم.*

[4] المرجع نفسه. (*دليل المساعدة القانونية المتبادلة وتسليم المجرمين* صفحة 19).

[5] قضية *لوكربي*، Joint Declaration of Judges Evensen, Tarassov, Guillaume and Aguilar Maudsley، تقارير محكمة العدل الدولية لسنة 1992، 3:24

[6] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012. *كتيب النقل الدولي للأشخاص المحكوم عليهم.* صفحة 23.

تعكس المعاهدات في العموم المبدأ الأساسي "للتسليم أو المقاضاة".[1] وعلى غرار ذلك، يُعمل عادة في شان إجراءات المساعدة القانونية المتبادلة بأحكام الاتفاقيات متعددة الأطراف – الإقليمية في الغالب[2] – أو الثنائية.[3] وقد تكون أحكام تسليم المجرمين والمساعدة القانونية المتبادلة بالمعاهدات "قائمة الذات" لتشير إلى سريانها على "المسائل الجنائية" في العموم،[4] أو مقيدة في نطاق شمولها في المعاهدة ذات الموضوع المحدد.[5]

ومتى كانت أي دولة طرفا في تلك الاتفاقيات، كثيرا ما ينص القانون الدولي على الإجراءات واجبة الاتباع في التعامل مع كل من الطلبات الواردة والصادرة. علاوة على ذلك، في بعض البلدان قد ينص القانون المحلي على أساس التعاون الدولي، بدلا من الاعتماد على أي معاهدة.[6] باعتبار أن أحد أهم أهداف المساعدة القانونية المتبادلة هو الحصول على الأدلة لتستخدم في المقاضاة والمحاكمات الجنائية، يرتبط هذا الإجراء ارتباطا وثيقا بقانون الإجراءات الجنائية الوطني. وسوف يحتاج تجميع الأدلة في الخارج – عادة بمعرفة الدولة الطالبة، وفي ظل الإجراءات التي تفرضها – إلى استيفاء قواعد الأدلة التي تفرضها الدولة متلقية الطلب. وقد يشمل هذا المعايير ذات الصلة بالإشاعات ومتابعة "سلسلة الاستحواذ"[7] على الأدلة. ومن أجل تنسيق الطلبات الصادرة والواردة لتسليم المجرمين والمساعدة القانونية المتبادلة، خصصت دول عدة "سلطة مركزية" ذات صلاحية لتلقي الطلبات وتنفيذها أو إرسالها إلى السلطات المختصة.[8] تتطلب المادة 18 من اتفاقية الجريمة المنظمة، على سبيل المثال، من الدول الأعضاء تخصيص سلطة مركبة لطلبات المساعدة القانونية المتبادلة.[9]

ويوجد بديل آخر للمساعدة القانونية المتبادلة وهو مبدأ *الاعتراف المتبادل* في مسائل التحقيق الجنائي. حيث تتطلب المساعدة القانونية المتبادلة مدة طويلة للتحقق من صحة الطلب – بما في ذلك ما يتعلق بما إذا كان

---

[1] أنظر اتفاقية الجريمة المنظمة، المادة 16(10).

[2] أنظر، على سبيل المثال، اتحاد دول جنوب شرق آسيا (آسيان)، 2004. *اتفاقية المساعدة القانونية المتبادلة في المسائل الجنائية*، مجلس أوروبا، 2000. *الاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية بين الدول الأعضاء في الاتحاد الأوروبي.*

[3] على سبيل المثال، الاتفاقية المبرمة بين حكومة المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية وحكومة جمهورية الأرجنتين بشأن المساعد القضائية المتبادلة لمكافحة الاتجار غير المشروع في المخدرات الموقعة بتاريخ 1991/08/27، تاريخ السريان 1994/06/01، معاهدة الولايات المتحدة وبنما بشأن المساعدة المتبادلة بالمسائل الجنائية، الموقعة بتاريخ 1991/11/04، تاريخ السريان 1995/06/09.

[4] أُنظر، على سبيل المثال، الاتفاقية بين الاتحاد الأوروبي واليابان بشأن المساعدة القانونية المتبادلة في المسائل الجنائية. OJ L 39/20. 12 شباط/فبراير 2010.

[5] أُنظر، على سبيل المثال، اتفاقية الأمم لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية لسنة 1998، المادة 7 التي تنص على *"تقدم الأطراف بعضها إلى بعض أكبر قدر من المساعدة القانونية المتبادلة في أي تحقيقات وملاحقات وإجراءات قضائية تتعلق بأية جريمة منصوص عليها في الفقرة 1 من المادة 3."*

[6] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012. *دليل المساعدة القانونية المتبادلة وتسليم المجرمين*، صفحة 22.

[7] المرجع نفسه، صفحة 15. أنظر أيضا الفصل السادس (الأدلة الإلكترونية والعدالة الجنائية).

[8] أُنظر استبيان دراسة الجريمة السيبرانية. السؤال رقم 195 (تسليم المجرمين) والسؤال رقم 217 (المساعدة القانونية المتبادلة).

[9] اتفاقية الجريمة المنظمة، المادة 18(13). سجل السلطات المختصة المعينة وفقا لاتفاقية الجريمة المنظمة وبروتوكولاتها، إضافة إلى اتفاقية الأمم لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية لسنة 1998، بالموقع www.unodc.org/compauth

التصرف محل الطلب جرما في ظل القانون المحلي للدولة متلقية الطلب.[1] يهدف الاعتراف المتبادل بين الدول إلى فرض إجراءات مبسطة وسريعة في ظل احتمالات محدودة لرفض الطلب، بناء على مبدأ الثقة المتبادلة في أنظمة العدالة الجنائية ووحدة القوانين. ويتطلب نجاح العمل به حدا أدنى من القوانين تتعلق بتحديد الجرائم والعقوبات الجنائية، إضافة إلى الاحتمالات المنسقة لحماية حقوق الفرد.[2] في السياق الأوروبي، يكون إطار المساعدة القانونية المتبادلة مصحوبا بالاتجاه الناشئ تجاه الاعتراف المتبادل – بما في ذلك من خلال تطوير أوامر الضبط والأدلة، ومقترحات "أوامر التحقيق الأوروبية".[3]

إضافة إلى صور التعاون الدولي الرسمي، يجوز إجراء أجزاء من تحقيقات إنفاذ القانون خارج الولاية القضائية بالاتصال غير الرسمي من الشرطة إلى الشرطة أو من وكالة إلى وكالة. ويمكن إجراء هذه الاتصالات *قبل* طلب التعاون القانوني المتبادل الرسمي إلى السلطة المختصة، أو *لتسهيل* الطلب غير الرسمي. ومتى استخدمت الشبكات الرسمية من الشرطة إلى الشرطة في مسائل مثل تحديد مكان الشهود أو المشتبه فيهم أو إجراء المقابلات أو مشاركة ملفات الشرطة أو وثائقها، يوجد مصدران للقلق، وهما: (1) عدم النظر في الطلب في الدولة متلقية الطلب في محاولة لإجراء تحقيقات جنائية أجنبية دون الحصول على الموافقة المناسبة، (2) استيفاء أي أدلة يجري الحصول عليها لتستخدم في المحاكمة لمعايير الأدلة في الدولة المطالبة، بما في ذلك متطلبات سلسلة الاستحواذ على الأدلة.[4]

إضافة إلى شبكة العلاقات الثنائية بين وكالات إنفاذ القانون، يحتفظ الإنتربول بنظام للمكاتب المركزية الوطنية في 190 بلد. وتعد هذه المكاتب أقساما مخصصة على نحو تقليدي مع وكالة إنفاذ القانون الوطنية.[5] ومن خلال نظام إلكتروني "I-24/7"، يجوز للمكاتب تسهيل الطلبات الثنائية أو متعددة الأطراف غير الرسمية من الشرطة إلى الشرطة، أو إرسال طلب المساعدة القانونية المتبادلة الرسمي من أي سلطة مركزية إلى أي سلطة مركزية أخرى – من خلال المكاتب المركزية الوطنية.[6]

---

[1] أنظر اتفاقية الجريمة المنظمة، المادة 18(9).

[2] في الإطار الأوروبي أنظر، على سبيل المثال، برنامج ستوكهولم OJ C115، 4 مارس 2010. 1-38.

[3] أنظر قرار إطار المجلس 2008/978/JHA المؤرخ 18 كانون الأول/ديسمبر 2008 بشأن أوامر الحصول على الأدلة الأوروبية لغرض الحصول على الأشياء والوثائق والبيانات لاستخدامها في إجراءات المسائل الجنائية، ومبادرة مملكة بلجيكا وغيرها بشأن أمر التحقيق الأوروبي في المسائل الجنائية. OJ C165/22. 24 حزيران/يونيو 2010. أنظر أيضا وكالة الاتحاد الأوروبي للحقوق الأساسية، 2011. *رأي وكالة الاتحاد الأوروبي للحقوق الأساسية بشأن مشروع التوجيه بشأن أمر التحقيق الأوروبي*.

[4] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012. *دليل المساعدة القانونية المتبادلة وتسليم المجرمين*، صفحة 66-76.

[5] أنظر http://www.interpol.int/About-INTERPOL/Structure-and-governance/National-Central-Bureaus

[6] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012. *دليل المساعدة القانونية المتبادلة وتسليم المجرمين*، صفحة 31.

ما هو "البعد عبر الوطني"؟

يتطلب المفهوم الشائع للجريمة السيبرانية المتضمن في "البعد" عبر الوطني التحليل بعناية. على سبيل المثال، متى وكيف يمكن القول أن أي جرم سيبراني يتضمن أي بعد عبر وطني؟ تتمثل نقطة الانطلاق في منظور اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة التي تنص على: يكون الجرم "ذا طابع عبر وطني" إذا: (أ) ارتُكب في أكثر من دولة واحدة، أو (ب) ارتُكب في دولة واحدة ولكن جرى جانب كبير من الإعداد أو التخطيط له أو توجيهه أو الإشراف عليه في دولة أخرى، أو (ج) ارتُكب في دولة واحدة، ولكن ضلعت في ارتكابه جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة واحدة، أو (د) ارتُكب في دولة واحدة، ولكن له آثار شديدة في دولة أخرى.[1]

يتضمن هذا المنظور العديد من السمات الهامة – بما فيها مبدأ "الآثار الشديدة" داخل الدولة. ولكن عندما يتعلق الأمر بالأفعال التي تنطوي على جريمة سيبرانية، قد لا يكون المنظور مكتملا. وكما يتناول هذا القسم "مرتكبو الجريمة السيبرانية" في الفصل الثاني (الصورة العالمية) من هذه الدراسة، لا توجد أي أسباب وراء تركيز "المجموعات الإجرامية المنظمة" على الأفعال التي تنطوي على جريمة سيبرانية.[2] علاوة على ذلك، ونظرا للحركة العالمية للبيانات في المعاملات الإلكترونية، قد يظهر "البعد" عبر الوطني" الذي قد لا يرتقي إلى "الإعداد أو التخطيط أو التوجيه أو التحكم" داخل أي دولة أخرى.

ويهدف منظور الجريمة السيبرانية إلى الاعتراف بأن تحديد "البعد" عبر الوطني يكون أكثر منطقية عند التحقق منه بالرجوع إلى اعتبارات (أ) *الولاية القضائية* و(ب) *الأدلة* الجنائية. ويتمثل أحد أساليب تحديد خصائص *أي* جرم، على سبيل المثال، في تمييز *عناصر* التصرف من "*فعل*"، "*ملابسات*"، "*نتيجة*".[3] ومتى حدث واحد أو أكثر من هذه العناصر، أو أدى إلى آثار شديدة"،[4] في ولاية قضائية إقليمية أخرى، وجد "البعد عبر الوطني". وعلى النحو الوارد أدناه، هذا سوف يكون له بدوره آثار على مطالبات الولايات القضائية. وفي ظل هذا

---

[1] اتفاقية الجريمة المنظمة، المادة 3(2).

[2] برغم تضمين عدد كبير في الواقع. أُنظر الفصل الثاني (الصورة العالمية)، القسم 2-3 مرتكبو الجرائم السيبرانية، دور مجموعات الجريمة المنظمة

[3] Fletcher, G., 1978. *Rethinking Criminal Law*. Oxford: Oxford University Press. على سبيل المثال، قد يتطلب أي جرم ينطوي على "تشويش على نظم الحاسوب" " غرض" (نية) "إحداث ضرر لبيانات الحاسوب أو إلغائها أو تغييرها أو قمعها" (الفعل) من أجل "إعاقة" (النتيجة) "عمل نظام الحاسوب" (الملابسات).

[4] قد أثير الجدل بشأن العمل "بمبدأ الآثار الجوهرية" على أنه يمثل امتداد لمبدأ الإقليمية الموضوعية، بقدر ما لا يتطلب وقوع أي "عنصر" من عناصر الجرم داخل نطاق الولاية القضائية. أُنظر، على سبيل المثال، *Ahlstrom and Others v Commission of European Communities* [1988] ECR 5193. وفي سياق الجريمة السيبرانية، تقترح المبادئ الولاية القضائية التي تعتمد المحاكم عليها في القضايا خارج الإقليم أن "*مهما كان التوصيف* [الإقليمية الموضوعية أو مبدأ الآثار الجوهرية] *التي تختار المحكمة المحلية أن تعتمد عليه، يكون نطاق الولاية القضائية المبرر هو نفسه*". أُنظر Hayashi, M., 2006. Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace. *In: Law* 6:284-302

المنظور قد يتعذر تحديد أي "موقع" للجرم السيبراني أو الوصول إليه في الواقع. وبالأحرى، ما يهم هو نجاح تحديد العناصر أو الآثار الشديدة التي تسمح لأي دولة بتحديد الولاية القضائية – وذلك دائما مع مراعاة متطلبات "الموصولية الكافية".

علاوة على ذلك، ومن منظور أوسع، قد ينشأ "البعد" عبر الوطني للجريمة السيبرانية متى وقع جزء من *أسلوب ارتكاب* الجرم في ولاية قضائية مختلفة. وقد لا يكون تزايد الخوادم خارج الإقليم لبيانات الحاسوب ذات الصلة بالجرم، على سبيل المثال، (بناء على القانون المحلي) كافيا لتضمين *الولاية القضائية* لبلد الخادم. وقد يكون الأمر، برغم ذلك، وثيق الصلة بالنسبة *للأدلة* وعملية التحقيق بأي بلد تطالب بالولاية القضائية، مما قد يتطلب اتخاذ إجراء مثل طلب المساعدة المتبادلة إلى بلد الخادم. وفي هذا الموقف، قد يمكن القول أيضا أن قضية الجريمة السيبرانبة لها "بعد" عبر وطني. وقد يقع عدد كبير من قضايا الجريمة السيبرانية في هذه الفئة. ولكن، لا يمكن وصفها دائما بذلك، إما لكفاية الأدلة في نطاق الولاية القضائية أو لتعذر الوصول للأدلة خارج الإقليم في المقام الأول.

ويوجد موضوعان على قدر من الأهمية الخاصة عندما يتعلق الأمر ببعد "الأدلة" خارج حدود الإقليم: (1) زيادة الأدلة الإلكترونية في جميع أنواع الجرائم وليس فقط في الجرائم التي تقع في نطاق مفهوم "الجريمة السيبرانية" و(2) زيادة استخدام الحوسبة السحابية التي تتضمن تخزين البيانات الموزعة والمتوازية. وعلى وجه الخصوص، قد يمثل استخدام البيانات الديناميكية المؤتمتة في نطاق الخدمات السحابية في مراكز البيانات تقع فعليا في بلدان مختلفة تحديات أمام تحديد "موقع" البيانات.[1] وبعد التعرف على كيفية تناول المنظورين الدولي والوطني للجوانب عبر الوطنية لجريمة السيبرانية عموما، يركز هذا الفصل خصوصا على الحصول على الأدلة خارج الإقليم من الأفراد ومقدمي الخدمات من الغير.

[1] أُنظر، على سبيل المثال، Peterson, Z.N.J., Gondree, M. and Beverly, R., 2011. A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud. *In: Proceedings of the ACM Conference on Data and Application Security and Privacy* (CODASPY). على سبيل المثال، تكنولوجيا استخدام البيانات المؤتمتة في مراكز البيانات الموزعة جغرافيا، أُنظر Agarwal, S., *et al.*, 2010. *Volley: Automated Data Placement for Geo-Distributed Cloud Services.* NSDI.

2-7 الولاية القضائية

الاستنتاجات الرئيسية:

- ينص القانون الدولي على عدد من قواعد الولاية القضائية فيما يخص أعمال الجريمة السيبرانية، بما في ذلك أشكال الولايات القضائية المستندة إلى الإقليم والمستندة إلى الجنسية
- وتوجد بعض هذه الأسس أيضا في الصكوك متعددة الأطراف المتعلقة بالجريمة السيبرانية.
- وهذا يشمل قضايا السيادة والولاية القضائية والتحقيقات عبر الوطنية والأدلة خارج حدود الولاية القضائية وأي من متطلبات التعاون الدولي
- وفي حين ترى كل البلدان الأوروبية أنَّ قوانينها الوطنية توفّر إطارا كافيا لتجريم الأفعال التي تندرج في عداد الجريمة السيبرانية والمرتكبة خارج نطاق الولاية القضائية ولملاحقة مرتكبيها قضائيا، فقد أبلغ نحو ثلث إلى نصف البلدان في مناطق أخرى من العالم عن عدم كفاية الأطر القائمة في هذا المجال
- وفي بلدان عديدة، تجسد الأحكام فكرة أنَّه ليس من الضروري أن تقع "كل عناصر" الجريمة داخل البلد من أجل تأكيد ولايته القضائية الإقليمية. ويمكن تحديد الروابط الإقليمية بالإشارة إلى عناصر الفعل المعني أو آثاره، أو موقع النظم أو البيانات الحاسوبية المستخدمة في ارتكابه للجريمة
- وتجري عادة تسوية تنازع الولايات القضائية من خلال المشاورات الرسمية وغير الرسمية بين البلدان
- ولا تكشف إجابات البلدان حاليا عن أي حاجة إلى أشكال إضافية من الولاية القضائية على بعد "فضاء سيبراني" مفترض، فغالبا ما تكون أشكال الولاية القضائية المستندة إلى الإقليم والمستندة إلى الجنسية قادرة دائما على ربط الجريمة السيبرانية المرتكبة ربطا كافيا بدولة واحدة على الأقل

ويتناول هذا القسم نهج الولاية القضائية لكل من صكوك وبلدان الجريمة السيبرانية الدولية والإقليمية. وكما هو مبين في الفصل الثالث من هذه الدراسة (التشريعات والأطر)، فإن عددا من الصكوك المتعلقة بالجريمة السيبرانية الدولية والإقليمية تحتوي على أحكام ولاية قضائية. وغالبا ما تحدد الصكوك أن الدول الأطراف تتبنى تدابير تشريعية وتدابير أخرى لتنص على أشكال معينة من الولايات القضائية على الجرائم القائمة وفقا للصكوك.[1] ويلخص الجدول أدناه أحكام الولاية القضائية في الصكوك الرئيسية الملزمة وغير الملزمة المتعلقة بالجريمة السيبرانية الدولية والإقليمية. وتم إدراج المزيد من التفاصيل وأرقام المقالات في الجدول في المرفق 3 في هذه الدراسة.

[1] أنظر على سبيل المثال: اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 22.

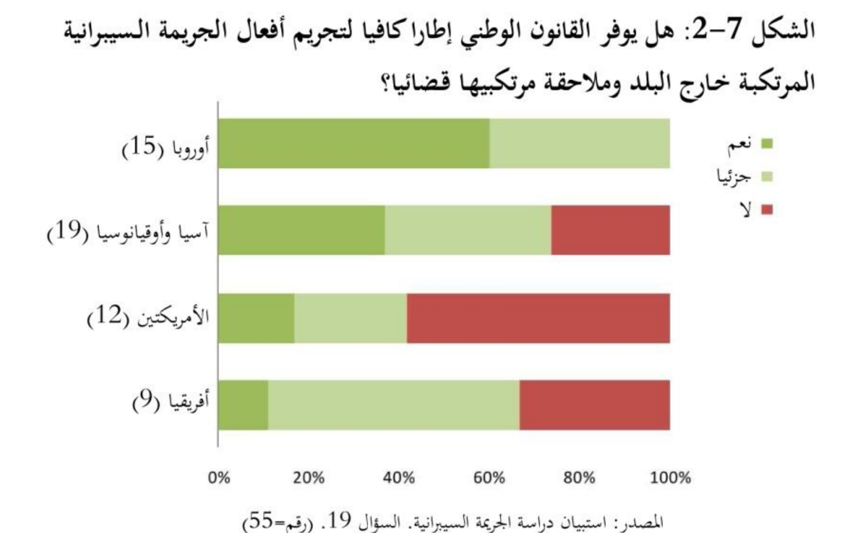
أحكام الولاية القضائية في الصكوك الدولية والإقليمية المتعلقة بالجريمة السيبرانية								
	صكوك ملزمة					صكوك غير ملزمة		
أسس الولاية القضائية	مشروع ميثاق الاتحاد الأفريقي	اتفاقية كومنولث الدول المستقلة	اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية	اتفاقية جامعة الدول العربية	اتفاقية منظمة شنغهاي للتعاون	مشروع الميثاق النموذجي لدول الكوميسا	مشروع الميثاق النموذجي لدول الكومنولث	الاتحاد الدولي للاتصالات، ومجموعة الكاريبي، والاتحاد الكاريبي للاتصالات
الولاية القضائية المستندة إلى الإقليم								
إقليمي	—	—	■	■	—	■	■	■
موجهة ضد الأنظمة الحاسوبية- البيانات في الإقليم	—	—	—	—	—	■	—	—
سفن/طائرات	—	—	■	■	—	■	■	■
الولاية القضائية المستندة إلى الجنسية								
نشط	—	—	■	■	—	■	■	■
سلبي	—	—	—	—	—	—	—	—
ولايات قضائية أخرى								
الإقامة الاعتيادية	—	—	—	—	—	—	—	—
مصالح الدولة	—	—	—	■	—	—	—	—
عند رفض تسليم المجرمين	—	—	■	■	—	■	—	—
أحكام إضافية								
قواعد بشأن الولايات القضائية المتزامنة	—	—	■	■	—	■	—	—

وتتم دراسة تفاصيل الأحكام الفردية أدناه إضافة إلى الأمثلة والممارسات ذات الصلة من المعلومات المستقاة من البلدان من خلال استبيان دراسة عن الجريمة السيبرانية.

الملاحقة القضائية للجرائم المرتكبة خارج الإقليم

خلال فترة جمع المعلومات لهذه الدراسة، سُئلت البلدان عن الكفاءة المتصورة لقوانينها الوطنية كإطار لتجريم الأفعال التي تندرج في عداد الجريمة السيبرانية والمرتكبة خارج نطاق االبلد ولملاحقة مرتكبيها قضائيا.[1] ويوضح الشكل 7-2 أن الصورة العامة هي إحدى الدرجات المعقولة من الكفاءة ولكن مع اختلافات إقليمية ملحوظة. إذ يعتقد حوالي ثلث إجمالي البلدان المجيبة عن الاستبيان أن الإطار القانوني الوطني للجرائم المرتكبة خارج الإقليم "كافٍ"، واعتبرته 40 في المائة من البلدان كافٍ "على نحو جزئي"، وأفادت 25 في المائة من البلدان أنه "غير كافٍ".[2] ويتوقع أن تكون الأطر أقل كفاءة في الأمريكتين حيث أفادت 40 في المائة فقط من البلدان أن الأطر القانونية الخاصة بها كانت غير كافية أو كافية جزئيا مقارنة بحوالي 67 في المائة من البلدان في أفريقيا وآسيا وأوقيانوسيا. واعتبرت كافة البلدان المجيبة عن الاستبيان من أوروبا – جميعها باستثناء بلد وقع أو صدق على اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية – أن تشريعاتها كافية بالكامل أو كافية جزئيا.

الشكل 7-2: هل يوفر القانون الوطني إطارا كافيا لتجريم أفعال الجريمة السيبرانية المرتكبة خارج البلد وملاحقة مرتكبيها قضائيا؟



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 19. (رقم=55)

استشهدت البلدان التي لم تعتبر تشريعاتها كافية للأفعال خارج أراضيها بعدد من الأسباب. وتضمنت الفجوات المشتركة إما الافتقار إلى الأحكام في القوانين الجنائية التي تتعامل مع الأفعال المرتكبة خارج الولاية القضائية، بالإضافة – في بعض الحالات – إلى عدم تطبيق تشريع تسليم المجرمين والمساعدة القانونية المتبادلة لأفعال الجريمة السيبرانية.[3]

---

[1] استبيان دراسة الجريمة السيبرانية، سؤال رقم 19.

[2] المرجع نفسه.

[3] المرجع نفسه.

وأفادت ردود البلدان المجيبة على استبيان الدراسة أن أسس الولاية القضائية في قضايا الجريمة السيبرانية خارج الإقليم مبنية على مبادئ مثل مبدأ الإقليمية (بما في ذلك ما يفسره مبدأ الإقليمية الموضوعي ومبدأ الآثار الإيجابية المستدامة) وجنسية مرتكب الجرم.[1] وعلى هذا المنوال، تطلب الدول في العموم درجة من التأثير الداخلي، مثل إلحاق الضرر بالمواطنين أو التسبب في وجود آثار أو أضرار داخل الإقليم. وكثيرا ما تفيد البلدان المجيبة أنه في حال ارتكاب جريمة *بالكامل* خارج البلد، دون أي تأثير داخل إقليمها، يمكن الطعن في إلحاق الضرر أو المقاضاة على وجه الخصوص.

الأسس الوطنية المشتركة للولاية القضائية في قضايا الجريمة السيبرانية

الإقليم

- ارتكاب الجريمة جزئيا أو كليا في الإقليم.
- الآثار/الأضرار داخل الإقليم
- الحاسوب/ البرمجة/ البيانات المستخدمة في ارتكاب الجريمة واقعة ضمن الإقليم
- ارتكاب الجريمة على متن السفن والطائرات المسجلة (بما فيها العسكرية)

الجنسية

- إيجابي – مرتكب الانتهاك
- معتاد الإقامة
- سلبي – المجني عليه

عوامل أخرى

- تأثر مصالح الدولة
- غير مكرر

استخدام الولاية القضائية الإقليمية

الصكوك الدولية والإقليمية – تحتوي جميع الصكوك الدولية والإقليمية على بند خاص بالولاية القضائية اعترافا بمبدأ الإقليمية – بما يتطلب من الدول الأعضاء ممارسة الولاية القضائية على أي جرم وفقا لهذا الصك والذي قد "يرتكب" في نطاق الإقليم الجغرافي للدولة.[2] كما تخضع الأنشطة الإجرامية على السفن والطائرات لعدد من الصكوك الملزمة وغير الملزمة.[3]

ووفقا لمبدأ الإقليمية الموضوعية، تعترف العديد من الصكوك الدولية والإقليمية أنه من غير الضروري وقوع جميع عناصر الجرم داخل الإقليم من أجل تطبيق الولاية القضائية الإقليمية. ويوضح التقرير التفسيري لاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، على سبيل المثال، أن في ظل مبدأ الإقليمية، يؤكد أي طرف على الولاية القضائية الإقليمية إذا وقع كل من الشخص الذي هاجم نظام الحاسوب ونظام المجني عليه في الإقليم الذي يتبعه،

[1] استبيان دراسة الجريمة السيبرانية، سؤال رقم 18 وسؤال رقم 19.

[2] أنظر، على سبيل المثال، اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 22(1)(أ)، اتفاقية جامعة الدول العربية، المادة 30(1)(أ)، البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال، المادة 4(1)، مشروع الميثاق النموذجي لدول الكوميسا، المادة 40(أ)(1)، نصوص القانون النموذجي للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 19(أ)، مشروع الميثاق النموذجي لدول الكومنولث، المادة 4(أ).

[3] أنظر، على سبيل المثال، مشروع الميثاق النموذجي لدول الكوميسا، المادة 40(ب)، مشروع الميثاق النموذجي لدول الكومنولث، المادة 4(ب)، اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 22(1)(ب) والمادة (ج)، اتفاقية مجلس أوروبا بشأن بحماية الطفل، المادة 25(1)(ب) والمادة (ج)، نصوص القانون النموذجي للاتحاد الدولي للاتصالات السلكية واللاسلكية/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، المادة 19(ب)، اتفاقية جامعة الدول العربية، المادة 30(1)(ب) والمادة (ج)، البروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال، المادة 4(1).

"*ومتى وقع نظام الحاسوب الذي تعرض للهجوم في الإقليم الذي يتبعه، حتى وإن لم يكن المهاجم خاضعا لهذا الإقليم*."[1]

مثال على التشريع السيبراني بشأن الولاية القضائية الإقليمية في قضايا الجريمة السيبرانية دولة في جنوبي أفريقيا

الولاية القضائية للمحاكم.

لأي محكمة في الجمهورية تجري محاكمة بشأن أي جرم بمقتضى هذا القانون ولاية قضائية في الحالات الآتية:

(أ) ارتكاب الجرم بالجمهورية؛

(ب) القيام بأي فعل للإعداد لارتكاب الجرم في الجمهورية أو أي جزء منه، أو متى أثرت أي نتيجة مترتبة على الجرم على الجمهورية؛

(ج) .....

(د) ارتكاب الجرم على متن أي سفينة أو طائرة مسجلة في الجمهورية أو في أي رحلة من الجمهورية أو إليها وقت ارتكاب الجرم.

وينص مشروع الميثاق النموذجي لدول الكوميسا على بند في الصك نفسه بشأن "*مكان وقوع الجرم*."[2] كما ينص أحد مكونات هذا البند على: "[ارتكاب جرم] ....(ب) في أي موقع حيث تكون النتيجة عنصرا من عناصر الجرم وفقا .... لهذا القانون قد وقعت أو يحتمل أن تقع."[3] ويتطلب توجيه الاتحاد الأوروبي بشأن استغلال الأطفال الولاية القضائية التي ارتكب فيها الجرم بالكامل "*أو جزء منه*" داخل الإقليم. وهو يوضح أن هذا يشمل الجرم المرتكب باستخدام تكنولوجيا المعلومات والاتصالات "*التي يجري الوصول إليها من*" الإقليم "*سواء*" كانت التكنولوجيا في الإقليم "*أم لا*".[4] ويغطي قرار الاتحاد الأوروبي بشأن الهجوم على نظم المعلومات بعض الهجمات التي يقوم بها مرتكب انتهاك موجود بالإقليم (سواء ضد نظام معلومات بالإقليم أم لا)، والهجمات مجددا على نظم المعلومات بالإقليم (سواء كان مرتكب الانتهاك موجود بالإقليم أم لا).[5]

النهج الوطنية– يظهر أثر النهج الإقليمية في الصكوك الدولية والإقليمية على المستوى الوطني. وقد أفادت البلدان بمجموعة من النصوص التي تعكس فكرة أن الجرم "بالكامل" لا يحتاج أن يرتكب داخل البلد لإقرار الولاية القضائية الإقليمية. وبرغم ذلك تعددت آليات تحديد وجود الصلة الإقليمية.

في بعض القضايا، يكون "التصرف" هو محل التركيز. وفي القضايا الأخرى، يكون موقع "نظم وبيانات الحاسوب" هو محل التركيز.[6] وقد أفادت بعض البلدان، على سبيل المثال، أن الولاية القضائية الإقليمية شملت

[1] مجلس أوروبا، 2001. *لتقرير التفسيري عن اتفاقية الجريمة السيبرانية*.
[2] مشروع الميثاق النموذجي لدول الكوميسا، المادة (40)(و).
[3] المرجع نفسه، المادة 40(و)(3).
[4] توجيه الاتحاد الأوروبي بشأن استغلال الأطفال، المادة 17.
[5] قرار الاتحاد الأوروبي بشأن الهجوم على نظم المعلومات، المادة 10.
[6] استبيان دراسة الجريمة السيبرانية. السؤال رقم 18.

الجرائم التي ارتكبت واستمرت واكتملت في مكان آخر، ولكنها "*ارتكبت*" جزئيا أو "*أثرت*" على الملكية أو أوقعت ضررا شخصيا داخل إقليم الدولة.[1] وأشارت بلدان أخرى إلى إقرار الولاية القضائية إذا "*استخدم أي خادم أو جهاز لارتكاب الجريمة*" خارج الإقليم، ولكن مع وجود "*أي أثر أو عنصر محلي*".[2]

ويوضح الاطلاع على قانون السوابق القضائية أن المحاكم الوطنية طالبت بالولاية القضائية على جميع *عناصر* أي جريمة في نطاق البلد، *باستثناء النتيجة* المترتبة (وفي هذه الحالة، الضرر الذي لحق بالمجني عليه خارج الحدود الذي يتلقى رسائل المضايقة).[3] والعكس بالعكس، عند إصدار سلطات إنفاذ القانون لاتهامات متى ترتبت على الجريمة *نتائج* (للوصول غير القانوني أو الخسارة الناتجة عن الاحتيال) داخل نطاق البلد، ولكن *سلوك* ومكان منتهكي الجرم كانا خارج الإقليم.[4] وقد لاحظت البلدان تطبيق هذه المفاهيم على القضايا التي تتضمن المقامر الإلكترونية واستغلال الأطفال في المواد الإباحية.[5] وقد أشار عدد صغير من بلدان أوروبا والأمريكتين، برغم ذلك، إلى عدم كفاية التشريع المحلي في التعامل مع بعض الأفعال التي تنطوي على جريمة سيبرانية خارج الإقليم – بما فيها قطع الخدمة، وإرسال الرسائل الطفيلية، والهجمات الاحتيالية.[6]

وقد أفادت بلدان عدة أنها لا تتمتع بالولاية القضائية على أي تصرف قد ارتكب، وله أثر، بالكامل خارج الإقليم. وقد أفادت إحدى بلدان آسيا، برغم ذلك، بإقرارها بالولاية القضائية في ظل هذه الظروف في حال استخدام نظم الحاسوب أو غيرها من المعدات في ارتكاب جرم خارج إقليمها.[7] وبينما يوجد فرق في المفاهيم بين "عناصر الجرم وآثاره"، و"نظم الحاسوب المستخدمة في ارتكاب الجرم"، يحتمل وجود تداخل ملحوظ بين النهجين – وخاصة إذا أمكن وصف استخدام نظم الحاسوب باعتباره جزءا من عناصر الجرم من "سلوك" أو "ملابسات".

وأخيرا، أحاطت بعض البلدان علما بقيود الجنسية على الإقليمية. وحتى في حال إمكانية إقرار الولاية القضائية – مثل حالة التصرف خارج الإقليم في ظل مبدأ الآثار الجوهرية – أفادت بلدان عدة بعدم وضوح الموقف إذا كان مرتكب الانتهاك خارج الإقليم مواطنا *أجنبيا*. وقد أحاطت العديد من البلدان علما بأنها لم تتخذ

---

[1] المرجع نفسه.

[2] المرجع نفسه.

[3] قضية *DPP v. Sutcliffe* [2001] VSC 43. 1 مارس 2001.

[4] قضية *US v Tsastsin* وآخرون، محكمة الولايات المتحدة الجزئية، المقاطعة الجنوبية لنيويورك S2 11 Cr. 878.

[5] استبيان دراسة الجريمة السيبرانية. السؤال رقم 18.

[6] استبيان دراسة الجريمة السيبرانية. السؤال رقم 19.

[7] استبيان دراسة الجريمة السيبرانية. السؤال رقم 18.

الإجراءات إلا عند استيفاء متطلبات إضافية.[1] وفي إحدى البلدان، على سبيل المثال، يعتمد تجريم المشتبه فيهم الأجانب ومقاضاتهم على ما إذا كان الجرم يوقع الضرر بمصالح هذا البلد والأمن الداخلي له.[2] بينما أفاد عدد قليل من بلدان آسيا والأمريكتين السماح بالولاية القضائية على مرتكبي الجرم من أي جنسية، بصرف النظر عن مكان ارتكاب الجرم نفسه – في حال وجود أي رابط، مثل وجود مرتكب الانتهاكات أو الجهاز أو البيانات المستخدمة في الجرم داخل الإقليم في الوقت المادي أو وقت وقوع الضرر داخل الإقليم.[3] وبالنسبة لحالة الادعاء بأي مرتكب الانتهاكات الأجنبي لا يزال موجودا بنفسه داخل الإقليم، أشارت بعض البلدان إلى التزامها "بتسليمه أو مقاضاته."

استخدام الولاية القضائية بناء على الجنسية

الصكوك الدولية والإقليمية – بينما تعترف جميع الصكوك الدولية والإقليمية بمبدأ الإقليمية، لكنها تنص تكرارا على مبدأ الجنسية الإيجابي – مما يتطلب من أي دولة التأكيد على الولاية القضائية عند القيام بالتصرف بمعرفة أحد مواطنيها، حتى وإن كان خارج الإقليم الوطني.[4] بينما تتطلب بعض الصكوك تجريم سلوك المواطن في البلد الذي وقع فيه التصرف.[5]

وينص عدد محدود من الصكوك على الولاية القضائية بناء على مبدأ الجنسية السلبي – مع الإشارة إلى ما يتناول منها حقوق الطفل. ويتطلب توجيه الاتحاد الأوروبي بشأن استغلال الأطفال والبروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال من الدولة تحديد ولاية قضائية على الجرم الذي يرتكب خارج الإقليم

مثال على تشريع لمد الولاية القضائية الإقليمية ليشمل غير المواطنين من دولة في الكاريبي:

(1) خاضع للقسم الفرعي (2)، هذا القانون فعال فيما يتعلق بأي شخص مهما كانت قوميته أو جنسيته، خارج وكذلك ضمن الدولة، وحيثما أرتكب جرم من قبل شخص في أي مكان خارج الدولة، قد يتم التعامل معه على اعتبار ارتكاب الجرم ضمن الدولة.

(2) لغاية القسم الفرعي (1)، هذا القانون يطبق إن، فيما يتعلق بالجرم المعني –

(أ) كان المتهم في الدولة وقتها؛

(ب) كان الحاسوب، أو البرنامج، أو البيانات في الدولة وقتها؛ أو

(ج) وقع الضرر ضمن الدولة، إن إنطبقت الفقرة (أ) والفقرة (ب) أو لم تنطبق.

---

[1] المرجع نفسه.

[2] المرجع نفسه.

[3] على سبيل المثال، أنظر قانون جرائم الحاسوب بماليزيا لسنة (1997)، المادة 9، وقانون إساءة استخدام الحاسوب بسنغافورة (نسخة منقحة لسنة 2007)، المادة 11، وقانون إساءة استخدام الحاسوب بترينيداد وتوباغو لسنة (2000)، المادة 12.

[4] أنظر، على سبيل المثال، اتفاقية مجلس أوروبا بشأن بحماية الطفل، المادة 25(1)(د)، وتوجيه الاتحاد الأوروبي بشأن استغلال الأطفال، المادة 17(1)(ب).

[5] مشروع الميثاق النموذجي لدول الكوميسا، المادة 40(ج)، ومشروع الميثاق النموذجي لدول الكومنولث، المادة 4(د)، واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 22(1)(د)، واتفاقية جامعة الدول العربية، المادة 30(1)(د).

ضد "أحد مواطنيه"، أو أي شخص "معتاد السكن فيه".[1] بينما تنص اتفاقية مجلس أوروبا بشأن بحماية الطفل على التزام الدول الأعضاء "بالسعي" لتحديد هذه ولاية قضائية.[2] وتقدم هذه الأحكام للبلدان سلطة الولاية القضائية لضمان حماية مواطنيها من الأطفال في الخارج.

النهج الوطنية – أشار عدد من البلدان إلى استخدام مبدأ الجنسية الإيجابي لإقرار الولاية القضائية على الجرائم التي يرتكبها مواطنوها، أينما كان مكان ارتكابها. ورغم أن هذا ليس بمتطلب شائع، أحاطت بضع بلدان علما بوجود متطلب ليتخذ التصرف صورة الجرم في الدولة التي يرتكب فيها.[3]

كما أشارت بضع بلدان إلى مبدأ الجنسية السلبي للولاية القضائية على الجرائم التي تؤثر على مواطنيها، أينما كان مكان وقوعها. وقد أفادت إحدى بلدان أوروبا، على سبيل المثال، أن العديد من قضايا الجريمة السيبرانية التي واجهتها تحتوي على عناصر خارج الإقليم، وأن في بعض الحالات يقع الموطنون المجني عليهم في الخارج – مما يترتب عليه تعقيدات تتصل بالولاية القضائية.[4] بينما أفادت إحدى بلدان أوروبا تبنّي قانون جنائي جديد ينص على مبدأ الجنسية السلبي على وجه الخصوص لتقليل الصعوبات إذا كان مرتكب الجرم أجنبيا وكانت الجريمة في الخارج وتؤثر على أي مواطن خارج الإقليم.[5]

استخدام أسس أخرى للولاية القضائية

الصكوك الدولية والإقليمية – ينص صكان (اتفاقية جامعة الدول العربية و مشروع الميثاق النموذجي) على وجه الخصوص على مبدأ الحماية، حيث تنص الاتفاقية، على سبيل المثال، على التزام الدول الأعضاء بمد اختصاصها ليشمل الجرائم التي تؤثر على "المصلحة العليا للدولة".[6] بينما تنص الصكوك الأوروبية، بما فيها قرار الاتحاد الأوروبي بشأن الهجوم على نظم المعلومات، على أساس إضافي للولاية القضائية على الجرائم التي ترتكب لصالح أي "شخصية اعتبارية" لها مقر بالإقليم.[7] وأخيرا، وفقا لمبدأ "تسليم المجرمين أو مقاضاتهم"، ينص عدد من

[1] توجيه الاتحاد الأوروبي بشأن استغلال الأطفال، المادة 17(2)(أ)، والبروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال، المادة 4(2)(ب).

[2] اتفاقية مجلس أوروبا بشأن بحماية الطفل، المادة 25(2).

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 18.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 19.

[5] المرجع نفسه.

[6] اتفاقية جامعة الدول العربية، المادة 30 (1)(هـ).

[7] قرار الاتحاد الأوروبي بشأن الهجوم على نظم المعلومات، المادة 10(1)(ج)، وتوجيه الاتحاد الأوروبي بشأن استغلال الأطفال، المادة 17(2)(ب)، وقرار الاتحاد الأوروبي بشأن الاحتيال والتزوير، المادة 9(1)(ج)، ومشروع توجيه الاتحاد الأوروبي بشأن الهجوم على نظم المعلومات، المادة 13(1)(ج).

الصكوك على الولاية القضائية على الإقليم الذي يوجد فيه مرتكب الانتهاك، وأن الدولة لا تسلمه إلى أي دولة أخرى إلا بناء على جنسيته وبعد طلب تسليمه.[1]

النهج الوطنية – أشارت بعض البلدان المجيبة إلى مبدأ الحماية في سياق الشروط المتصلة بجميع صور الولاية القضائية، وبالنسبة لأسس الولاية القضائية الأخرى، مثل الولاية القضائية العالمية، أشار عدد من البلدان إلى حالة ارتكاب جرم خارج الإقليم بالكامل بمعرفة أجنبي موجود في الإقليم دون تقديم طلب لتسليمه. وقد أحاطت بعض البلدان علما بأن الولاية القضائية العالمية كانت مقتصرة على الجرائم الدولية الحقيقية، وأنها لم تشمل في العموم الأفعال التي تنطوي على جرائم سيبرانية.[2] بينما اقترح آخرون أن بعض الأفعال الخطرة التي تنطوي على جرائم سيبرانية، مثل استغلال الأطفال في المواد الإباحية، تقع في نطاق هذه الولاية القضائية.[3]

إختلافات الولايات القضائية

الصكوك الدولية والإقليمية– يمكن أن يؤدي عمل مجموعة من قواعد الولاية القضائية بمعرفة دول مختلفة إلى حالة تؤكد فيها أكثر من دولة الولاية القضائية على أفعال معينة تنطوي على جريمة سيبرانية. وتتعامل مجموعة من الصكوك الدولية والإقليمية مع هذا التحدي المتمثل في الولاية القضائية "المشتركة". وعلى سبيل المثال، يقوم البعض بتخصص الأمر بحيث أنه عندما تقع مخالفة ضمن الولاية القضائية لأكثر من دولة وعندما تقوم أي دولة من الدول المعنية بالمحاكمة على نحو صحيح وبناء على الوقائع، فإنه يتعين على الدول أن "تتعاون" أو "تتشاور" لتقرير الولاية القضائية الأنسب للمقاضاة.[4] وتهدف الصكوك الأوروبية على وجه التحديد إلى "تمركز الإجراءات القضائية في [دولة] واحدة".[5] وتنص اتفاقية الدول العربية على ترتيب أولويات مفصلة لطلبات الولايات القضائية المتعارضة على النحو التالي: (1) الدول التي يتعرض أمنها أو مصالحها لخطر نتيجة هذا الجرم. (2) الدول التي تُرتكب فيها الجريمة. (3) الدولة التي يحمل مرتكب الجريمة جنسيتها. في حالة عدم وجود رصيد وفق هذه الترتيب، فتكون الأولوية لأول دولة طالبة.[6]

---

[1] مشروع الميثاق النموذجي لدول الكوميسا، المادة 40(د)، واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 22(3)، واتفاقية مجلس أوروبا بشأن بحماية الطفل، المادة 25(7)، وقرار الاتحاد الأوروبي بشأن الهجوم على نظم المعلومات، المادة 10(3)، وقرار الاتحاد الأوروبي بشأن الاحتيال والتزوير، المادة 10(1)، واتفاقية جامعة الدول العربية، المادة 30 (2)، والبروتوكول الاختياري لاتفاقية حقوق الطفل بشأن بيع الأطفال، المادة 4(3).

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 18.

[3] المرجع نفسه.

[4] اتفاقية مجلس أوروبا لحماية الطفل، المادة 25 (8)؛ اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 22 (5)، قرار الاتحاد الأوروبي بشأن الهجمات ضد نم المعلومات، المادة 10 (4)؛ مشروع قانون الكوميسا المادة 40 (هـ)

[5] أنظر على سبيل المثال قرار الاتحاد الأوروبي حول الهجمات ضد نظم المعلومات، المادة 10(هـ).

[6] اتفاقية الدول العربية، المادة 30(هـ).

الأساليب الوطنية – أثناء جمع المعلومات الخاصة بالدراسة، أفادت البلدان بشكل عام بعدم تمتعها بتشريعات محددة تهدف لحل اختلافات الولايات القضائية في حالات الجريمة السيبرانية.[1] ومع ذلك، أشار عدد من البلدان إلى خطط لمعالجة اختلافات الولايات القضائية المحتملة في تشريعات سيبرانية معينة عن طريق الاستقصاءات القانونية أو المواقف السياسية. وعلى الرغم من ذلك، أشارت إحدى الدول إلى أنه بقدر القلق من الجريمة السيبرانية عبر الوطنية فإن "نطاق الحالات والسيناريوهات المحتملة ربما يجعلها صعبة ولذلك لا ينصح بتطوير قواعد قانونية عالمية مادية على أساس خصوصية الولايات القضائية".[2]

أفادت البلدان بحل اختلافات الولايات القضائية من خلال الاعتماد على المشاورات الرسمية وغير الرسمية مع الدول الأخرى وذلك لتجنب التحقيقات المزدوجة وتنازع الولايات القضائية.[3] وأشارت إحدى الدول في أوروبا إلى أنه "*غالبا ما يمكن تجنب اختلافات الولايات القضائية من خلال المشاورات المسبقة غير الرسمية أو التبادل التلقائي للمعلومات. ويمكن أن تساهم عمليات التحقيق المشترك في [...].*"[4] ويكون الاتصال إما بشكل ثنائي أو عبر قنوات تتيحها مؤسسات مثل الإنتربول ويوروبول ويوروجست.[5] وأشارت إحدى الدول من الأمريكتين إلى أنه بما أن ملاحقة الجرائم المجزئة صعبة جدا، فإن إجراءات التقاضي يمكن أن تبدأ عند وجود إشارة قوية إلى أن المتهم أو الضحية أحد مواطنيها. ويتم التواصل بخصوص جميع الحالات الأخرى مع بلدان المنشأ عبر قنوات الإنتربول.[6] بالإضافة إلى إشارة عدد من الدول إلى مبدأ عدم جواز محاكمة الشخص على ذات الجرم مرتين، بحيث تبدأ الإجراءات القضائية في حال عدم القيام بها في البلد الذي ارتكبت فيه تلك الأفعال. وقبل التسليم لها بمطالبتها بشأن الولاية القضائية، تطلب بعض الدول تأكيدات بأن تلتزم الدولة الأخرى، التي تدعي الولاية القضائية، بمعايير حقوق الإنسان أثناء التحقيقات وأثناء التقاضي.[7]

ولاية قضائية وافية؟

وبشكل عام، يشير تحليل الصكوك الدولية والإقليمية فضلا عن قانون الدول وممارستها إلى أنه يمكن حل تحديات الولاية القضائية للجريمة السيبرانية من خلال تأكيد وضوح المبادئ القائمة وتطبيقها المبتكر.

ويسلط المعلقون الضوء على أن "*المعاملات التي تجري في الفضاء الإلكتروني تتضمن أشخاصا حقيقيين في إحدى الولايات القضائية الإقليمية إما من خلال (1) التعامل مع أشخاص حقيقيين في ولايات قضائية إقليمية أو (2) الانخراط في نشاط في إحدى الولايات القضائية التي تسبب تأثيرات واقعية في ولاية قضائية إقليمية*

[1] الاستبيان الخاص بالدراسة، السؤال رقم 18

[2] المرجع نفسه.

[3] المرجع نفسه

[4] المرجع نفسه.

[5] المرجع نفسه.

[6] المرجع نفسه.

[7] استبيان دراسة الجريمة السيبرانية. السؤال رقم 19.

أخرى".[1] ونتيجة لذلك، دائما ما استطاعت الأنماط الإقليمية والولاية القضائية القائمة على الجنسية ضمان أنه يمكن إقامة "علاقة وافية" أو "رابطة حقيقية" بين الأفعال التي تنطوي على جريمة سيبرانية وإحدى الدول على الأقل. لذلك لا تجد هذه الدراسة حاجة، في الوقت الراهن، لمزيد من الولاية القضائية ذات بعد يتعلق بـ "الفضاء الإلكتروني". وتقع الغالبية الساحقة من الأفعال التي تنطوي على جريمة سيبرانية ضمن الفئتين المذكورتين أعلاه كما يمكن ربطها بدول محددة. وإذا كان الأمر كذلك فضلا عما نوقش لاحقا في هذا الفصل، تمثل البيانات المؤقتة والمتفرقة عبر مراكز البيانات العالمية المزيد من التحدي لجمع الأدلة أكثر منه فما يتعلق بتقرير الولاية القضائية. وللحد الذي يمكن *لعناصر وتأثيرات* التصرف الفردي المنطوي على جريمة سيبرانية أن تكون جميعها مؤقتة ومتفرقة، من الممكن أن تظل أشكال الولاية القضائية معتمدة على مبادئ قائمة على الجنسية (الأشخاص الاعتباريين)، ومحل مبادئ التأسيس.

وكما نوقش في الفصل الرابع (التجريم) في إطار القانون الدولي لحقوق الإنسان فإنه من الممكن أن يكون أحد مخاطر عرض المزيد من الولاية القضائية الإقليمية هو التأثير على تعدد محتوى الإنترنت. ويكمن في قلب النقاش الخاص بالولاية القضائية تفسير وضع عناصر الجرم وآثاره داخل الحدود الجغرافية. وسواء تم النظر إليها من منظور "الأفعال" أو "السلوك" أو "الظروف" أو "البيانات" أو "النظم الحاسوبية"، فإن تجنب اختلافات الولايات القضائية يعتمد على الإبقاء على مستوى مرتفع بشكل كافي من "رابطة حقيقية"، مع قنوات اتصال واضحة بين الدول من أجل التنسيق في إجراءات العدالة الجنائية التي تتجاوز حدود الولاية القضائية.

[1] Post, D.G., 2002. Against 'Against Cyberanarchy.' Berkeley Technology Law Journal(17):1365-1387.

3-7 التعاون الدولي أ - التعاون الرسمي

الاستنتاجات الرئيسية:

- نظرا لطبيعة الأدلة الإلكترونية المتقلبة، يتطلب التعاون الدولي في الأمور المتعلقة بالجريمة السيبرانية استجابة مناسبة فضلا عن القدرة على طلب إجراءات تحقيق متخصصة
- ويسود استخدام أنماط التعاون الدولي التقليدية للحصول على أدلة تتجاوز حدود الولاية القضائية في حالات الجريمة السيبرانية. وأفاد أكثر من 70 في المائة من الدول المجيبة باستخدام طلبات المساعدة القانونية المتبادلة والرسمية لهذا الغرض
- وضمن هذا التعاون الدولي، تستخدم ما يقرب من 60 في المائة من الطلبات صكوك ثنائية بوصفها الأساس القانوني. وتُستخدم الصكوك متعددة الأطراف في 20 في المائة من الحالات
- وتفيد التقارير أن أوقات الاستجابة الخاصة بالآليات الرسمية تكون بناء على ترتيب الشهور لكلٍ من طلبات تسليم المجرمين والمساعدة القانونية المتبادلة
- وتوجد قنوات عاجلة لطلبات المساعدة القانونية المتبادلة في بعض البلدان، لكن لا يتضح تأثير هذه القنوات على أوقات الاستجابة
- والصورة الحالية للتعاون الدولي تهدد ظهور مجموعات البلدان التي تحظى بصلاحيات وإجراءات ضرورية للتعاون فيما بينها، إلا أنها مقيدة لجميع البلدان الأخرى بأنماط التعاون الدولي "التقليدية" التي لا تراعي خصوصيات الأدلة الإلكترونية

ويتناول هذا القسم آليات التعاون الدولي في الأمور المتعلقة بالجريمة السيبرانية الموجودة في الصكوك الدولية فضلا عن القوانين والممارسات الوطنية.

أحكام التعاون في الصكوك الدولية والإقليمية

وكما نوقش في الفصل الثالث (التشريعات والأطر) من هذه الدراسة، يحتوي عدد من صكوك الجريمة السيبرانية الدولية والإقليمية على أحكام التعاون الدولي. فعادة ما تحتوي الصكوك إما على التزامات عامة واسعة على الدول الأطراف لتتعاون[1] أو آليات تعاون محددة، بما في ذلك تسليم المجرمين[2] والمساعدة القانونية المتبادلة[3].

[1] اتفاق كومنولث الدول المستقلة، المادة 5، اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 23، اتفاقية منظمة شنغهاي للتعاون، المادة 3-5. ويشير مشروع اتفاقية الاتحاد الأفريقي إلى المبدأ الموجود في المادة 3 (14).

[2] مسودة قانون كوميسا النموذجية، المادة 42 (ج)؛ اتفاقية مجلس أوروبا لحماية الطفل، المادة 38 (3)؛ قرار الاتحاد الأوروبي بشأن الاحتيال والتزييف، المادة 10.

[3] اتفاق كومنولث الدول المستقلة، المادة 6؛ اتفاقية مجلس أوروبا لحماية الطفل، المواد 25، 27؛ التوجيه المقترح للجماعة الاقتصادية لدول غرب أفريقيا، المادة 35؛ اتفاقية جامعة الدول العربية، المواد 32، 34.

ويلخص الجدول أدناه أحكام التعاون الدولي في صكوك الجريمة السيبرانية الدولية والإقليمية الرئيسية الملزمة وغير الملزمة. ويتضمن الجدول في الملحق 3 من هذه الدراسة المزيد من التفاصيل وأعداد المادة.

أحكام التعاون في الصكوك الدولية والإقليمية المتعلقة بالجريمة السيبرانية								
	صكوك ملزمة					صكوك غير ملزمة		
أحكام التعاون الدولي	مشروع اتفاقية الاتحاد الأفريقي	اتفاقية كومنولث الدول المستقلة	اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية	اتفاقية جامعة الدول العربية	اتفاقية منظمة شنغهاي للتعاون	مسودة قانون كوميسا النموذجية	قانون الكومنولث النموذجي	النصوص التشريعية النموذجية للاتحاد الدولي للاتصالات، ومجموعة الكاريبي، والاتحاد الكاريبي للاتصالات
التعاون الدولي العام								
مبدأ التعاون الدولي العام	■	■	■	—	■	■	—	—
تسليم جرائم الصكوك	—	—	■	■	—	■	—	—
المساعدة القانونية المتبادلة العامة	—	■	■	■	—	■	—	—
مساعدة محددة								
مساعدة عاجلة	—	■	■	■	—	■	—	—
حفظ بيانات الحاسوب	—	—	■	■	—	■	—	—
مصادرة بيانات الحاسوب/ الوصول إليها/ وجمعها والإفصاح عنها	—	—	■	■	—	■	—	—
أشكال أخرى من التعاون								
الوصول عبر الحدود	—	—	■	■	—	■	—	—
شبكة 7/24	—	—	■	■	—	■	—	—
أحكام إضافية								
متطلبات التجريم المزدوج	—	—	■	■	—	■	—	—

ويعتبر نطاق التعاون أحد نقاط الانطلاق الرئيسية في دراسة هذه الأحكام. وفي حين أنه عادة ما تشير أحكام الولاية القضائية في الصكوك الدولية والإقليمية إلى جرائم معينة منشأة بموجب الصك، فإن أحكام التعاون الدولي إما أن "تعمل" على الجرائم ذاتها أو تحظى بنطاق أوسع.

ويبين فحص الصكوك الخمسة الملزمة أن أحكام التعاون الدولي تحظى في جميع الصكوك بنطاق متعلق بـ "الجريمة السيبرانية" أو المفاهيم وثيقة الصلة مثل "الجرائم المتعلقة بمعلومات الحاسوب" أو "المعلومات وجرائم

تكنولوجيا المعلومات". بالإضافة إلى قيام صكين (اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية واتفاقية جامعة الدول العربية) بتمديد أحكام المساعدة القانونية المتبادلة لجمع الأدلة الإلكترونية في أي جرم. وكما ذُكر في الفصل السادس (الأدلة الإلكترونية والعدالة الجنائية)، ويحظى هذا بأهمية في إطار الدور المتزايد للأدلة الإلكترونية في التحقيقات والمقاضاة في جميع أشكال الجريمة. ويتم في هذا الفصل بحث آثار مثل تلك التغيرات في نطاق التعاون الدولي.

الصك	مجال صكوك التعاون الدولي
مشروع اتفاقية الاتحاد الأفريقي	• "الجريمة السيبرانية"
اتفاقية كومنولث الدول المستقلة	• "الجرائم المتعلقة بالمعلومات الحاسوبية"
اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية	• "الجرائم الجنائية المتعلقة بنظم الحاسوب والبيانات" • "جمع أدلة الجريمة الجنائية في شكل إلكتروني"
اتفاقية جامعة الدول العربية	• "المعلومات وجرائم تكنولوجيا المعلومات" • "جمع الأدلة الإلكترونية في الجرائم"
اتفاقية منظمة شنغهاي للتعاون	• "أمن المعلومات الدولي"

ويتعين وضع آليات التعاون المتضمنة داخل صكوك الجريمة السيبرانية الدولية والإقليمية في إطار تعاون دولي أوسع. وعلى الرغم من أن عددا من الصكوك يمكن الاعتماد عليها بوصفها أساس قانون لأعمال تعاون معينة،[1] إلا أنه يتعين تذكر أن الدول الأطراف في الصكوك هي طرف أيضا في شبكات أوسع من الاتفاقيات الثنائية ومتعددة الأطراف المتعلقة بالتعاون في المسائل الجنائية، بما في ذلك المعاهدات مثل اتفاقية الجريمة المنظمة. وبناء على طبيعة التصرف الذي يخضع للتحقيق، فإنه من الممكن أن تقع احتياجات التعاون ضمن مجموعة من الآليات القانونية. وتميّز بعض صكوك الجريمة السيبرانية هذه المسألة. وتنص اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية على سبيل المثال على تعاون الأطراف مع بعضها بعضا، ليس فقط "*وفق أحكام هذا الفصل*" وإنما أيضا "*من خلال تطبيق الصكوك الدولية ذات الصلة على التعاون الدولي في الأمور الجنائية، وخلال الاتفاق على الترتيبات القائمة على التشريعات الموحدة والمتبادلة فضلا عن القوانين المحلية*".[2]

وأخيرا فإنه من المهم التأكيد على أن الصكوك غير الملزمة لا يمكنها تقديم الأساس القانوني الدولي نفسه فيما يتعلق بالتعاون بالقدر الذي تقدمه الصكوك الملزمة. وعلى سبيل المثال، فإنه على الرغم من أن مسودة قانون كوميسا النموذجية تحدد أن "السلطات القانونية [لهذه الدولة] تتعاون مباشرة وبأكبر مدى ممكن مع السلطات

[1] أنظر على سبيل المثال اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المواد 24 وما يليها؛ اتفاقية جامعة الدول العربية، المواد 31 وما يليها؛ اتفاق كومنولث الدول المستقلة، المواد 6 وما يليها؛ مسودة قانون كوميسا النموذجية، المواد 42 وما يليها.

[2] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 24.

القانونية لدولة أخرى"،[1] إلا أن هذا يمثل مجرد نص يقترح إدراجه في القانون الوطني. وحتى عند إدراج مثل هذا النص، فإن الدول عموما لا تزال بحاجة إلى آلية سياسية قانونية – سواء كانت معاهدة متعددة الأطراف أو ثنائية، أو تفاهم متبادل– مع الدول الطالبة. وفي هذا الصدد، يتعين الإشارة إلى إتباع بعض الدول لسياسة "الباب المفتوح" للتعاون التي بموجبها يمكن القانون الوطني من التعاون مع أي دولة.[2]

تسليم المجرمين والمساعدة القانونية المتبادلة في الصكوك الدولية والإقليمية

يعتبر الصكان الملزمان اللذان تم تضمينهم في الجدول أعلاه (اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية واتفاقية جامعة الدول العربية)، وصك غير ملزم (مسودة قانون كوميسا النموذجية) تسليم المجرمين عن الجرائم الواردة فيها على وجه التحديد.[3] وكل تلك الأمور تجعل تسليم المجرمين معتمدا على الوصف الجنائي للجرم وخطورته. وتقدم ثلاثة من الصكوك الملزمة (اتفاق كومنولث الدول المستقلة، واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، واتفاقية جامعة الدول العربية) فضلا عن مسودة قانون "كوميسا" النموذجية المساعدة القانونية المتبادلة.[4] وتعتبر بعض الصكوك أن طلبات المساعدة القانونية المتبادلة من الممكن أن تخضع للوصف الجنائي المزدوج.[5] وتحدد الصكوك أيضا أنه من الممكن رفض تلك الطلبات عندما يُنظر إلى التنفيذ باعتباره "مخالفا للتشريعات الوطنية"،[6] و"يتعلق الطلب بالجريمة السياسية"،[7] أو أن الطلب "من المحتمل أن يمس السيادة أو الأمن أو النظام العام أو المصالح الأساسية الأخرى".[8]

كما تقدم الصكوك أيضا وسائل اتصالات عاجلة، مثل البريد الإلكتروني والفاكس، وذلك للطلبات العاجلة،[9] مع وجود البعض الذي يطلبون درجة "معقولة" من الأمن لمثل تلك الاتصالات وطلب متابعة مكتوبة خلال فترة زمنية معينة.[10] وأخيرا، تشمل اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية واتفاقية جامعة الدول العربية نصوصا معينة حول طلبات المساعدة القانونية المتبادلة وذلك لـ: (1) الحفاظ العاجل لبيانات الحاسوب المخزنة؛ (2) الإفصاح العاجل عن بيانات المرور المحفوظة؛ (3) المساعدة المتبادلة في التحصيل الفوري لبيانات

[1] مسودة قانون كوميسا النموذجية، المادة 41.

[2] أشارت بعض الدول المجيبة إلى وجود مثل تلك السياسات (دراسة الجرائم السيبرانية. السؤال رقم 220).

[3] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 24؛ اتفاقية جامعة الدول العربية، المادة 31؛ مسودة قانون كوميسا النموذجية، المادة 42 (ج).

[4] اتفاق كومنولث الدول المستقلة، المادة 6، اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 25، 27؛ اتفاقية جامعة الدول العربية، المواد 32، 34؛ مسودة قانون كوميسا النموذجية، المواد 43 (أ)، 45.

[5] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 24 (1)، 25 (5)، اتفاقية جامعة الدول العربية، المواد 32 (5)، 37 (3) و (4)؛ مسودة قانون كوميسا النموذجية، المواد 42 (أ)، 43 (د).

[6] أُنظر على سبيل المثال، مسودة قانون كوميسا النموذجية، المادة 45 (ج)(1).

[7] أُنظر على سبيل المثال، اتفاقية جامعة الدول العربية، المادة 45.

[8] أُنظر على سبيل المثال، اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 27 (4)(ب).

[9] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 23 (3)؛ اتفاقية جامعة الدول العربية، المادة 32 (3).

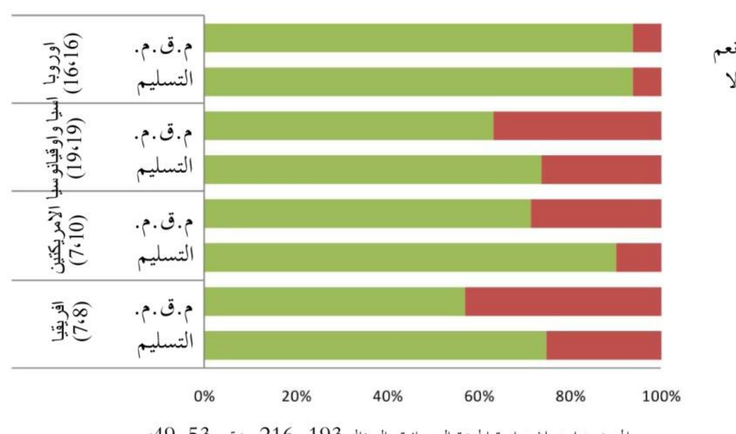
[10] اتفاق كومنولث الدول المستقلة، المادة 6 (2).

المرور؛ (4) المساعدة المتبادلة فيما يتعلق باعتراض بيانات المحتوى.[1] وبسبب النطاق الواسع لأحكام التعاون الدولي المتعلقة بتلك الصكوك، لا تنطبق أشكال المساعدة المتخصصة فقط على الجرائم المتعلقة بالحاسوب، ولكن أيضا على الجرائم بشكل عام.[2]

استخدام آليات التعاون في حالات الجريمة السيبرانية

فعلى مستوى التشريعات الوطنية، أفاد أكثر من ثلثي البلدان في أفريقيا وأسيا وأوقيانوسيا، والأمريكتين بوجود التشريعات الوطنية التي تنطبق على تسليم مرتكبي الجريمة السيبرانية وأمور المساعدة القانونية المتبادلة. وأفادت جميع البلدان في أوروبا تقريبا بوجود مثل تلك التشريعات. وعادة ما تكون التشريعات السارية الخاصة بتسليم المجرمين أكثر من تلك الخاصة بالمساعدة القانونية المتبادلة.[3] ويشير تحليل التشريعات الذي استشهدت به البلدان إلى أن الغالبية الساحقة من تلك القوانين ليست محددة بالجريمة السيبرانية، لكنها تغطي تسليم المجرمين والمساعدة القانونية المتبادلة في الأمور الجنائية العامة.[4] وينبغي الإشارة إلى أن غياب التشريعات الوطنية حول تسليم المجرمين والمساعدة القانونية المتبادلة لا تمنع البلدان بالضرورة من الانخراط في التعاون الدولي في الأمور المتعلقة بالجريمة السيبرانية. فعلى سبيل المثال، يمكن التعامل مع الأمور المتعلقة بالتعاون الدولي بموجب الآليات الوطنية مثل الأوامر التنفيذية أو السياسات الإدارية.

الشكل 7-3: **وجود تشريع للتسليم والمساعدة القانونية المتبادلة (م.ق.م) في قضايا الجريمة السيبرانية**



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 193 و216. (رقم=53، 49)

[1] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المواد 29-31، 34؛ اتفاقية جامعة الدول العربية، المواد 37-39، 41، 42.

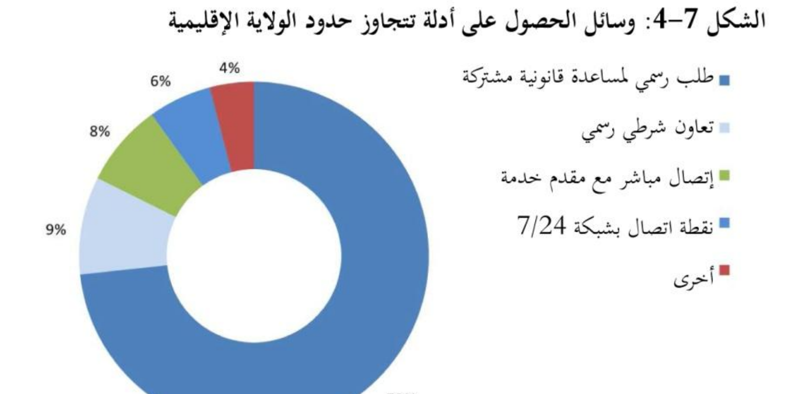
[2] على الرغم من الإشارة إلى التحصيل الفوري لبيانات المرور واعتراض بيانات المحتوى، فإنهس ينبغي تقديم المساعدة فقط وفق المدى الذي يسمح به القانون المحلي.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 193 ورقم 216.

[4] المرجع نفسه.

ويغلب استخدام آليات التعاون الرسمي في حالات الجريمة السيبرانية عبر الوطنية على أشكال التعاون الأخرى. ويبين الشكل 7-4 أن أكثر من 70 في المائة من سلطات تنفيذ القانون أفادت بأن المساعدة القانونية المتبادلة الرسمية تستخدم للحصول على مجموعة من أنواع الأدلة بصورة أكبر من الولايات القضائية الأخرى.[1] وأفادت التقارير أن الآليات الأقل استخداما تشمل التعاون غير الرسمي بين أجهزة الشرطة، والاتصال المباشر مع مزود خدمة، فضلا عن استخدام نقاط اتصال 24/7.[2]

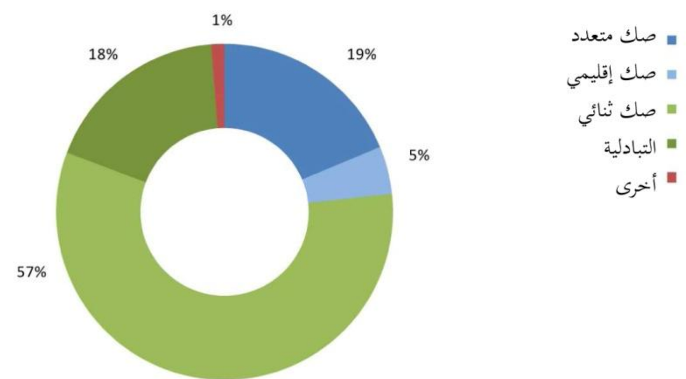
الشكل 7-4: **وسائل الحصول على أدلة تتجاوز حدود الولاية الإقليمية**



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 105. (رقم=56، 221)

وفي إطار مثل هذا التعاون الرسمي، يعتبر استخدام الصكوك الثنائية الخاصة بالجريمة السيبرانية أمرا شائعا جدا. فقد أفادت 60 في المائة تقريبا من البلدان باعتمادها على الصكوك الثنائية بوصفها الأساس القانوني لتسليم المجرمين والمساعدة القانونية المتبادلة في حالات الجريمة السيبرانية.[3] وذكر 20 في المائة التبادلية بوصفها الأساس. وعلى الرغم من أن حوالي 60 في المائة من البلدان التي أجابت على الاستبيان الخاص بالدراسة وقعت أو أقرت اتفاق الجريمة السيبرانية الدولية أو الإقليمية بما في ذلك

الشكل 7-5: **الأساس القانوني لتسليم مرتكبي الجريمة السيبرانية وطلبات المساعدة القانونية المتبادلة**



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 202-207 و227-232. (رقم=21، 50)

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 105.

[2] المرجع نفسه.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 202-207. كانت نسبة البلدان التي أجابت على تلك الأسئلة المحددة التي وقعت أو أقرت صكوك الجريمة السيبرانية الدولية أو الإقليمية مثل تلك النسبة الخاصة بجميع الدول المجيبة.

أحكام التعاون،[1] كانت 25 في المائة فقط من تلك الحالات صكوكا دولية وإقليمية تم ذكرها باعتبارها الأساس القانوني.[2]

ويعتبر عدد من البلدان التي أجابت على الأسئلة الخاصة بالأساس القانوني للتعاون منخفضا نسبيا. لذلك ينبغي ترجمة النتائج بحذر. وعلى الرغم من أن الاستخدام الغالب للصكوك الثنائية والتبادلية يعكس: (1) أنه ليست جميع البلدان طرفا في الصكوك متعددة الأطراف؛ (2) استخدام الأنماط "التقليدية" للتعاون الدولي، حتى عندما تكون البلدان طرفا في الصكوك متعددة الأطراف. وفي هذا الصدد، لم تذكر أي دولة وجود صكوك ثنائية محددة بالجريمة السيبرانية، ولم يتم تحديد أي منها في سياق بحوث الدراسة.

وربما لا يمثل استخدام الأنماط "التقليدية" للتعاون صعوبات عندما تستخدم بين البلدين التي هي *أيضا* طرف في الصكوك متعددة الأطراف. ومن المحتمل أن تستطيع البلدان طلب إجراءات تحقيق متخصصة للجرائم السيبرانية، مثل تلك الخاصة بحفظ بيانات الحاسوب حيث سيحظى الطرفان بصلاحيات إجرائية ذات صلة في القانون الوطني. على الرغم من التحديات التي يمثلها استخدام الأنماط "التقليدية" التي *لا* تكون فيها إحدى البلدان طرفا في الصكوك متعددة الأطراف. وهذا هو الحال بالنسبة لغالبية البلدان في العالم. وعالميا فإن أكثر من 60 في المائة من البلدان ليست طرفا في صك الجريمة السيبرانية متعددة الأطراف مع نتيجة مفادها أن هذه الدول ليس لديها التزام قانوني دولي سواء لإدارج صلاحيات التحقيق المتخصصة للجرائم السيبرانية ضمن قوانينها الإجرائية الوطنية، ولا القيام بتحقيقات متخصصة ردا على طلبات التعاون.[3]

وعلى سبيل المثال، أفادت 20 في المائة من الدول المجيبة أن التشريعات الوطنية لا تقدم حفظا عاجلا لبيانات الحاسوب.[4] وكما هو متوقع، لم توقع غالبية (80 في المائة) تلك البلدان أو تقر أيا من صكوك الجريمة السيبرانية الدولية والإقليمية. وينبغي حاليا عمل تلك الطلبات الخاصة بالتعاون الدولي لتلك البلدان من خلال الوسائل "*التقليدية*" الثنائية والقائمة على التبادلية. لكن في حال طُلبت بعض الأعمال مثل الحفظ العاجل للبيانات، فإنه من الممكن أن يعاني الطلب من: (1) نقص الوضوح فيما يتعلق بما إذا كان من الممكن طلب مثل تلك التدابير بموجب صك ثنائي مناسب أو ترتيبات أو (2) عدم وجود مثل تلك التدابير بموجب القانون الوطني للإجراءات الجنائية.

[1] الموقعون والدول الأطراف باتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة (40 في المائة)، اتفاقية جامعة الدول العربية (10 في المائة)، اتفاق كومنولث الدول المستقلة (15 في المائة)، اتفاقية منظمة شنغهاي للتعاون (10 في المائة). وتصل الأرقام لأكثر من 60 في المائة نظرا لعضوية الصكوك المتعددة بالنسبة لبعض البلدان.

[2] استبيان دراسة الجريمة السيبرانية. الأسئلة رقم 202-207 والأسئلة رقم 227-232.

[3] على الرغم من الإشارة إلى ذلك في الفصل الخامس (إنفاذ القانون والتحقيقات) إلا أنهم سيستفيدون من صلاحيات التحقيق العامة القائمة.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 49.

الوصف الجنائي المزدوج والشروط الأخرى في التعاون المتعلق بالجريمة السيبرانية

ويمكن أن يمثل استخدام التعاون الدولي للتحقيق في أعمال الجريمة السيبرانية تحديا فيما يتعلق بتكافؤ التجريم. وعادة ما تخضع طلبات التعاون إلى مجموعة من المتطلبات الإجرائية والموضوعية حيث يتعين رضا الدولة متلقية الطلب عليها قبل منح الموافقة. وأحد المتطلبات الرئيسية هي تلك التي تتعلق *بالوصف الجنائي المزدوج*. ويتطلب المبدأ الخاص بالوصف الجنائي المزدوج أن يكون التصرف المتعلق به الطلب جريمة وفق القانون الجنائي للدولة متلقية الطلب وكذلك للدولة الطالبة.[1] ملامح الوصف الجنائي المزدوج في صكوك الجريمة السيبرانية الدولية والإقليمية. فهي من الأمور المطلوبة لتسليم المجرمين والمتصورة لأشكال المساعدة القانونية المتبادلة على سبيل المثال بموجب اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية واتفاقية جامعة الدول العربية.[2]

أحد العوامل في تقرير الوصف الجنائي المزدوج هو السلوك الأساسي الموضوعي وليس المصطلحات أو التعريفات الفنية للجرم في القوانين الوطنية.[3] وتوضح اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية أن الوصف الجنائي المزدوج سيكون مستوفى "*بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن نفس فئة الجرائم أو تستخدم في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف الطالبة*"، إذا "*كان السلوك الذي يقوم عليه الجرم*" الذي تلتمس بشأنه المساعدة "*يعتبر فعلا إجراميا في قوانينها*".[4] ووفقا لهذا النهج، يكون التركيز على "تحويل" عناصر التصرف إلى قانون الدولة متلقية الطلب من أجل التأكد من أن التصرف من شأنه أيضا أن يكون جريمة جنائية.[5]

يمكن تجريم بعض أفعال الجريمة السيبرانية بشكل واضح في أحد البلدان وليس في آخر، ولذلك يفشل اختبار الوصف الجنائي المزدوج. فإنتاج أدوات إساءة استخدام الحاسوب فضلا عن توزيعها أو امتلاكها ليس مجرّما

---

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012. *دليل بشأن المساعدة القانونية المتبادلة وتسليم المجرمين*. لا يعتبر الوصف الجنائي المزدوج قاعدة من قواعد القانون الدولي العرفي مثل المعاهدة والنظام الأساسي القائمة على السياسة والملائمة (وليامز، إس.إيه، 1991. قاعدة الوصف الجنائي المزدوج وتسليم المجرمين: تحليل مقارن. مراجعة قانون نوفا، 15: 582).

[2] يمكن أن تجد إشارات إلى هذا المفهوم في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المواد 24 (1)، 25 (5)، 29 (3)، و (4)؛ اتفاقية جامعة الدول العربية، المواد 32 (5)، 37 (3)، و (4).

[3] على سبيل المثال، تنص المادة 43 (2) من اتفاقية الأمم المتحدة لمكافحة الفساد على أنه: "*في مسائل التعاون الدولي، كلما اشترط توافر الوصف الجنائي المزدوج وجب اعتبار ذلك الشرط مستوفى بصرف النظر عما إذا كانت قوانين الدولة الطرف متلقية الطلب تدرج الجرم المعني ضمن نفس فئة الجرائم أو تستخدم في تسميته نفس المصطلح الذي تستخدمه الدولة الطرف الطالبة، إذا كان السلوك الذي يقوم عليه الجرم الذي تلتمس بشأنه المساعدة يعتبر فعلا إجراميا في قوانين كلتا الدولتين الطرفين.*"

[4] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 25 (5).

[5] يوجد نهجان في هذا الصدد: الوصف الجنائي المزدوج نظريا والوصف الجنائي المزدوج من حيث ماهيته. فتعني نظريا أن النظر في السلوك الذي نحن بصدده يقتصر على مسألة ما إذا كان السلوك يعاقب عليه بصرف النظر عن المؤهل القانوني أو وجود الأسباب الممكنة التي تمنع المعاقبة. ومن حيث ماهيتها تعني أن السلوك يستوفي جميع متطلبات المعاقبة، بما في ذلك غياب أي مبرر مثل الدفاع عن النفس، أو العذر أو أسباب أخرى تمنع المعاقبة. (أنظر مجلس أوروبا اللجنة الأوروبية المعنية بمشاكل الجريمة، 2012. ملاحظات على الوصف الجنائي المزدوج، نظريا ومن حيث الماهية، لجنة الخبراء الخاصة بالاتفاقيات الأوروبية حول التعاون في المسائل الجنائية (2012) 02 النهائي، 11 مايو 2012.)

في 20 في المائة من البلدان التي أجابت على الاستبيان الخاص بالدراسة.[1] وستواجه الطلبات المتعلقة بهذا الجرم الموجه لتلك البلدان تحديات الوصف الجنائي المزدوج.

مثال لتشريع مخصص بالجريمة السيبرانية بشأن التعاون الدولي أصدره بلد في غرب أفريقيا

حفظ البيانات الحاسوبية والإفصاح العاجل عنها ضمن التعاون الدولي

(1) يمكن أن يطلب من [الدولة] الإسراع في حفظ البيانات المخزنة على نظام الحاسوب الموجود في [الدولة]، مع الإشارة إلى الجرائم المنصوص عليها في هذا القانون، ووفقا لتسليم الطلب الخاص بالمساعدة في تفتيش تلك البيانات وحجزها والكشف عنها.

(2) ...

(3) خلال تنفيذ طلب سلطة أجنبية بموجب الأجزاء السابقة، فإنه يجوز للنائب العام للاتحاد أن يصدر أمرا بحفظ تلك البيانات لأي شخص يتحكم في هذه البيانات أو تتوافر لديه، بما في ذلك مزود الخدمة.

(4) إلى (6) ...

(7) يمكن رفض الطلب الخاص بالإسراع في حفظ بيانات الحاسوب إذا كان ثمة أسباب معقولة تفضي للاعتقاد برفض طلب المساعدة القانونية للتفتيش اللاحق لتلك البيانات وكذلك حجزها وإصدارها نظرا لعدم التحقق من الوصف الجنائي المزدوج.

وبخصوص الأفعال المجرّمة على نطاق واسع عبر البلدان مثل الأفعال المتعلقة بالحاسوب والتي تسبب ضررا شخصيا، فإن الكثير من الاختلافات الدقيقة التي نوقشت في الفصل الرابع (التجريم) لن تشكل عائقا أمام إنشاء الوصف الجنائي المزدوج. وعلى الرغم من ذلك، فإنه بناء على النهج الذي تتبعه السلطات الوطنية في إجراءات التعاون مثل جلسات استماع تسليم المجرمين، يمكن أن تكون الاختلافات في تجريم أفعال الجريمة السيبرانية أمرا مناسبا. وفي بعض البلدان، يمكن أن تُعتبر أمور مثل "استخدام الوسائل الفنية" لارتكاب جريمة (في حالة الاعتراض غير القانوني) أو "حدود" الإهانة (في حالة جرائم المحتوى) عناصر مكونة للجريمة، الأمر الذي يعني أنه لا توجد جريمة ما لم تكن تلك العناصر موجودة. وفي مثل تلك الظروف، يمكن أن تنشأ بشكل مشروع تحديات أمام الوصف الجنائي المزدوج. وأشارت إحدى البلدان المجيبة إلى تحديات الوصف الجنائي المزدوج في حالة جرائم حقوق التأليف والنشر المتعلقة بالحاسوب والاحتيال الحاسوبي، مع الإشارة وفق البلد متلقية الطلب أنه لا يوجد جرم مكافئ للذي هو موضوع الطلب.[2]

بالإضافة إلى أن الوصف الجنائي المزدوج يمكن أن يلعب دورا هاما في طلبات المساعدة القانونية المتبادلة،[3] بما في ذلك تعلق تدابير المساعدة بجمع الأدلة الإلكترونية الخاصة بـ "أي جرم" (بدلا من "جريمة سيبرانية" معينة أو جرائم "متعلقة بالحاسوب"). وعلى سبيل المثال تتيح اتفاقية مجلس أوروبا المتعلقة بالجريمة

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 28.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 215.

[3] فيما يتعلق بالتعاون الجنائي بشكل عام، يمكن أن يتراوح الوصف الجنائي المزدوج للمساعدة القانونية المتبادلة من كونها غير مطلوبة على الإطلاق إلى كونها مطلوبة لبعض الأفعال القسرية الخاصة بالمساعدة القانونية المتبادلة فضلا عن كونها مطلوبة لأي نوع من أنواع المساعدة القانونية المتبادلة. (أنظر مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2012. *دليل بشأن المساعدة القانونية المتبادلة وتسليم المجرمين*).

السيبرانية للدول الأطرف إمكانية تطبيق متطلبات الوصف الجنائي المزدوج على الطلبات الخاصة بحفظ بيانات الحاسوب.[1] وتصبح الأدلة الإلكترونية المتفرقة جغرافيا هامة بشكل متزايد بالنسبة للتحقيقات الجنائية "التقليدية" للحد الذي يصبح فيه الوصف الجنائي المزدوج مطلوبا بوصفه بحثا رئيسيا. فمن ناحية أفاد عدد من البلدان بحاجتها إلى وجود وصف جنائي مزدوج، عندما تكون التدابير المطلوبة "تدخلا بشكل خاص"، مثل التفتيش أو الحجز أو التنصت أو المراقبة.[2] من ناحية أخرى، يلعب الوصف الجنائي المزدوج دورا هاما في حماية سيادة الدولة وإنفاذ قانونها فضلا عن شؤون العدالة الجنائية. ويمكن أن يقدم الوصف الجنائي المزدوج، على سبيل المثال، أساسا قانونيا للبلدان لرفض طلبات منح الأدلة الإلكترونية المتعلقة بجرائم الإنترنت المتعلقة بالمحتوى وغير المجرمة في البلد متلقية الطلب. وفي الحالات التي تتضمن المساعدة القانونية المتبادلة ومحتوى الإنترنت بشكل خاص، توضح القواعد الإضافية للرفض، مثل استثناءات الجريمة السياسية، استثناءات المصالح الأساسية،[3] ويمكن الاستعانة بالالتزامات الدولية لحقوق الإنسان.[4] وفي الواقع، عند السؤال عن الأسباب الشائعة لرفض طلبات المساعدة القانونية المتبادلة المتعلقة بالجريمة السيبرانية، فقد كشفت بعض الدول المجيبة تحديدا عن "*خرق لالتزامات حقوق الإنسان*".[5]

وأخيرا، فبالإضافة إلى قضية وجود جريمة جنائية في قانون الدولة متلقية الطلب، فإن الكثير من الصكوك الثنائية ومتعددة الأطراف تنشأ مستويات *جدية* لطلبات التعاون الدولي.[6] ويتم إدراج المستويات على سبيل المثال في اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية واتفاقية جامعة الدول العربية، حيث تنص الاتفاقيتان على تسليم المجرمين على الجرائم المقررة وفق الاتفاقية "*والمعاقب عليها بموجب قوانين كلا الطرفين*" (متطلب الوصف الجنائي المزدوج) من خلال "*الحرمان من الحرية ... لمدة عام على الأقل، أو بعقوبة أشد*" (معيار المستوى).[7] وخلال جمع المعلومات الخاصة بالدراسة، أفادت البلدان بأن الأفعال التي تنطوي على الجريمة السيبرانية تلبي بشكل كبير معايير الجدية وبالتالي تشكل جرائم يمكن تسليم مرتكبيها. وأفادت جميع البلدان في أوروبا والأمريكتين و 90 في المائة من البلدان في أفريقيا وأسيا وأوقيانوسيا بأن الأفعال التي تنطوي على الجريمة السيبرانية هي بشكل عام جرائم يمكن تسليم مرتكبيها.[8]

[1] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 28 (4). لاحظ أن طلبات المساعدة القانونية المتبادلة في الاتفاقية تنطبق على الجرائم الجنائية المتعلقة بالحاسوب والبيانات وكذلك جمع أدلة الجريمة الجنائية في صورة إلكترونية.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 198.

[3] أنظر على سبيل المثال، اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 29(4).

[4] أنظر على سبيل المثال، كوري، أر. جي، 2000. حقوق الإنسان والمساعدة القانونية المتبادلة الدولية: حل التوترات. *منتدى القانون الجنائي*، 11 (2): 143-181.

[5] استبيان دراسة الجريمة السيبرانية. السؤال رقم 239.

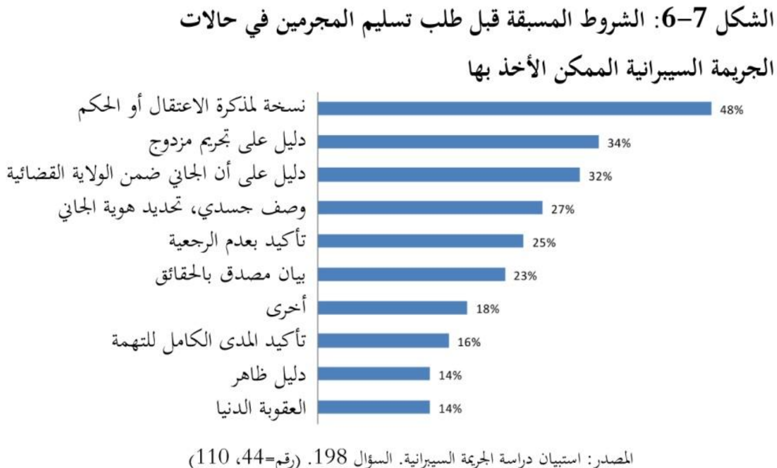
[6] أنظر على سبيل المثال، تفاقية الجريمة المنظمة، المواد 2، 3، و 16.

[7] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 24.

[8] استبيان دراسة الجريمة السيبرانية. السؤال رقم 194.

وأظهرت بلدان قيودا على الوصف الجنائي المزدوج عندما سئلت عن "الشروط المسبقة" لطلبات التعاون في الجريمة السيبرانية. ويمكن اعتبار تلك الشروط بأن لديها طبيعة إجرائية وطبيعة موضوعية، ويمكن أن تختلف نظرة البلدان للشروط المختلفة.[1] ففي حين أفادت بلدان بكلٍ من العناصر الإجرائية والموضوعية إلا أنه تم تحديد الوصف الجنائي المزدوج بوصفه متطلب لكلٍ من تسليم المجرمين والمساعدة القانونية المتبادلة.[2] في حال تسليم المجرمين، حددت البلدان أيضا متطلبات الإجراءات المتوقعة مثل نسخة من مذكرة التوقيف أو حكم المحكمة فضلا عن الدليل على أن المشتبه به ضمن الولاية القضائية.[3] وفي حال المساعدة القانونية المتبادلة، حددت البلدان شروطا مثل التأكيدات الخاصة بكفاية الأدلة المطلوبة وبيان وقائع موثق.[4]

الشكل 7-6: الشروط المسبقة قبل طلب تسليم المجرمين في حالات الجريمة السيبرانية الممكن الأخذ بها



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 198. (رقم=44، 110)

وعلى الرغم من إشارة عدد من البلدان إلى أنها لم ترفض تسليم أي مرتكبين للجرائم السيبرانية أو ترفض طلب مساعدة حتى الآن إلا أن البلدان أكدت عدم تلبية المتطلبات الإجرائية والموضوعية عندما سئلت عن الأسباب الشائعة لرفض الطلبات.[5] وأفادت البلدان كثيرا بمخالفات إجرائية وعدم كفاية الأدلة، الأمر الذي يؤكد الحاجة لإعداد دقيق لطلبات التعاون.[6] وقدمت الأسباب الموضوعية وصفا جنائيا مزدوجا يحظى باهتمام فضلا عن التزامات القانون الدولي لحقوق الإنسان.[7] ومن الجدير بالذكر أن إحدى البلدان أفادت بمشكلة عملية تتعلق بـ "*سرعة تأثر بيانات الحاسوب*" بوصفها سببا لرفض طلبات المساعدة القانونية المتبادلة،[8] وربما تشير إلى الطلبات التي لا يمكن استيفائها باعتبارها دليلا إلكترونيا تم حذفه بالفعل. ويرتبط هذا بشكل وثيق بالوقت المطلوب للرد على الأشكال الرسمية للتعاون، وهذه قضية تم تناولها أدناه.

---

[1] بالنسبة لتسليم المجرمين، يمكن على سبيل المثال اعتبار نسخة مذكرة التوقيف والوصف المادي للمشتبه به عناصر إجرائية تخضع للفحص الأولي الخاص "بالامتثال للقواعد النظامية". ومن ناحية يمكن النظر بعمق في وجود الوصف الجنائي المزدوج عند جلسة استماع تسليم المجرمين أمام السلطة القضائية (رد من خبير إقليمي ترشحه دول أوروبا الغربية ودول أخرى على النتائج الأولية التي تم استخلاصها من الدراسة).

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 198 و السؤال رقم 220.

[3] المرجع نفسه.

[4] المرجع نفسه.

[5] استبيان دراسة الجريمة السيبرانية. السؤال رقم 214 و السؤال رقم 239.

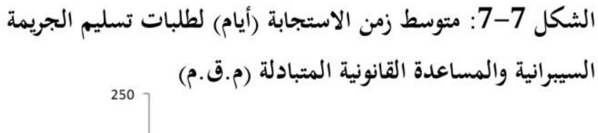
[6] المرجع نفسه.

[7] المرجع نفسه (السؤال 239).

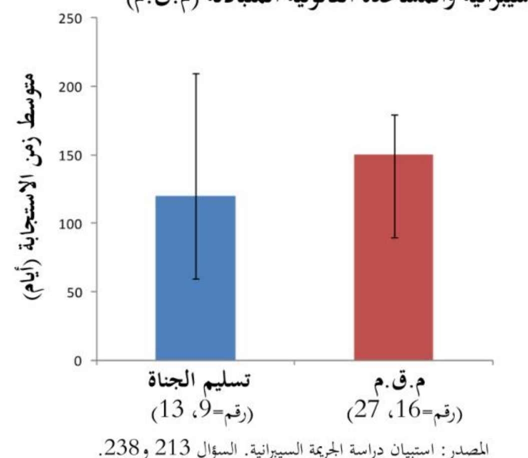
[8] المرجع نفسه (السؤال 239).

تسليم المجرمين والمساعدة القانونية المتبادلة في الواقع العملي

أوضحت الإحصاءات المتاحة من خلال الاستبيان بخصوص هذه الدراسة أن البلدان تستخدم تسليم المجرمين والمساعدة القانونية بحدود متفاوتة، وأفاد حوالي نصف الدول المجيبة أن أقل من 10 حالات تسليم مجرمين أو مساعدة قانونية متبادلة في جرائم سيبرانية مرسلة أو مستلمة سنويا.[1] وكان الرقم المتوسط للحالات 8 سنويا، على أن ثلاثة أرباع البلدان المجيبة تقع في مدى 3 إلى 45 حالة سنويا. وكانت الدول ذات أعلى عدد من الحالات هي الدول الأكبر في أوروبا أو أمريكا الشمالية.



الشكل 7–7: متوسط زمن الاستجابة (أيام) لطلبات تسليم الجريمة السيبرانية والمساعدة القانونية المتبادلة (م.ق.م)



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 213 و238.

يتشابه توزيع الجريمة السيبرانية الخاضعة لطلبات تسليم المجرمين والمساعدة القانونية المتبادلة مع إجمالي القضايا التي تتعامل معها سلطات إنفاذ القانون في العموم – بما يمثل حوالي ثلث الأفعال التي تضر بسرية نظم أو بيانات الحاسوب وسلامتها وإتاحتها، والأفعال التي يترتب عليها ربح أو ضرر شخصي أو مالي، والأفعال ذات الصلة بالمحتوى.[2] تشمل التدابير الأكثر شيوعا لمطالبة الدول بالتحقيق في هذه الأفعال تقديم المحتوى المخزن أو بيانات نسبة استخدام الشبكة، أو البحث عن أجهزة وبيانات حاسوبية أو احتجازها.[3] وفقا لحقيقة أن بعض البلدان لا تتمتع بسلطات تحقيق متخصصة، مثل حفظ بيانات الحاسوب أو الزمن الفعلي لتجميع بيانات الاتصال أو نسبة استخدام الشبكة في القوانين الوطنية، أفادت حوالي 35 في المائة و45 في المائة من البلدان، على التوالي، بأن هذه الإجراءات يمكن طلبها من خلال المساعدة القانونية المتبادلة.[4]

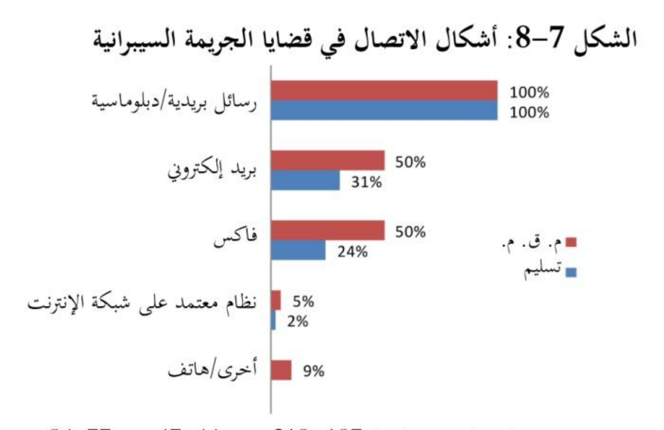
وبينما يتسع مدى الجرائم المشمولة، وسلطات التحقيق المتاحة من خلال التعاون الدولي الرسمي، إلا أن الاستجابة لهذه الآلية قد تستغرق زمنا أطول في الواقع العملي. وقد بلغ متوسط زمن الاستجابة 120 يوما

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 202–206 والسؤال رقم 227–231.
[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 208–211 والسؤال رقم 233–236.
[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 221.
[4] المرجع نفسه.

لطلبات تسليم المجرمين، 150 يوما لطلبات المساعدة القانونية المتبادلة المستلمة منها والمرسلة.[1] وينبغي دراسة البيانات مع توخي الحذر نظرا للعدد المنخفض جدا من البلدان التي تستجيب للطلب، ونظرا لاحتمال تطبيق البلدان لمجموعة من تعريفات الإطار الزمني استجابة للطلب – على سبيل المثال، من "استلام الطلب" حتى "الاستجابة المبدئية"، أو من "استلام الطلب" حتى التوصل إلى "قرار موضوعي". ومع الأخذ في الاعتبار أن 75 في المائة من جميع أزمنة الاستجابة المذكورة تقع في إطار خط "شريط الخطأ"،[2] ولكن يتضح أن استخدام آليات التعاون الدولي تحدث في إطار زمني يمتد لأشهر، وليس أياما.

وقد ترتبط الأطر الزمنية الطويلة في التعاون الدولي بالاعتماد على قنوات الاتصال الرسمية "التقليدية" التي تحتاج إلى دخول العديد من السلطات في سلسلة الاتصال. وقد أفادت جميع البلدان، على سبيل المثال، استخدام البريد أو الخطابات الدبلوماسية في طلبات تسليم المجرمين والتعاون الدولي المتبادل في قضايا الجريمة السيبرانية.[3] هذا بينما سلط عدد من البلدان الضوء على أن أسلوب تقديم الطلبات تنظمه أحكام المعاهدة الثنائية أو الاتفاقية متعددة الأطراف ذات الصلة. وفي بعض الحالات، تشمل هذه المعاهدات أو الاتفاقيات أنماط رسمية من الاتصالات.[4]

الشكل 7-8: أشكال الاتصال في قضايا الجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 197 و219. (رقم=44، 47، رقم=77، 94)

وعادة ما تتطلب آليات التعاون الرسمي تحديد "السلطات المركزية" – وهي تلك السلطات التي تتعامل بصورة تقليدية مع الطلبات الواردة والصادرة بالبريد أو بخطاب دبلوماسي. اتفاقية كومنولث الدول المستقلة، على سبيل المثل تتطلب من الدول الأعضاء إعداد "*قائمة بالسلطات المختصة*."[5] بينما تتطلب اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية تحديد السلطات المختصة المركزية المختصة بتسليم المجرمين والمساعدة القانونية المتبادلة.[6] وبما أن قضايا الجريمة السيبرانية

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 213 والسؤال رقم 238.
[2] أشرطة الخطأ على الشكل تمثل الأرباع ذات القيم العليا والدنيا.
[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 197 والسؤال رقم 219.
[4] المرجع نفسه.
[5] اتفاقية كومنولث الدول المستقلة، المادة 4.
[6] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 24 والمادة 27. السلطات المختصة المخطر عنها في ظل هذه المواد مذكورة على:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp

يجري التعامل معها على نطاق واسع على غرار قضايا الجرائم الأخرى، أفادت البلدان بالمؤسسات التقليدية التي يسند إليها دور السلطة المركزية من أجل مسائل التعاون بشأن الجريمة السيبرانية.[1] وهي تشمل النائب العام أو المدعي العام ووزارات العدل.[2] وأحاطت بعض البلدان علما بإسناد دور السلطة المركزية لسلطات مختلفة بناء على مراحل الإجراءات.[3] وبينما تتحمل السلطة المركزية المسؤولية عن تنسيق أي طلب، فإن *القرار* النهائي بشأن أي طلب غالبا ما يكون لسلطة وطنية مختلفة.[4] فبالنسبة لبلدان أوروبا، على سبيل المثال، طلبات التصريح لا يجري التعامل معها بانتظام – بدءا من قرار المحكمة المحلية الدنيا إلى قرار الفرع التنفيذي للحكومة.[5] وفي الأقاليم الأخرى، يضطلع المدعون والقضاة بدور هام. ويمكن للتفاعل (كلما دعت الضرورة) بين مجموعة المؤسسات الحكومية، في بعض القضايا، المساهمة في طول الأطر الزمنية للاستجابة للطلبات.

وكما ركز الفصل الخامس (الأدلة الإلكترونية والعدالة الجنائية)، فالأدلة الإلكترونية سريعة التأثر وقد لا توجد إلا لفترات زمنية قصيرة – وفي كثير من الحالات، تكون الفترات الزمنية أقصر مما أفادته الدول عاليه. وقد سلط عدد من البلدان المجيبة الضوء، على سبيل المثال، بأن: "*يمكن أن تستهلك آليات التعاون الدولي الرسمية مثل المساعدات القانونية المتبادلة الوقت، وأن تتسبب في تأخير التحقيق والمحاكمة بشأن الجريمة السيبرانية.*"[6] ونادرا ما تحتوي القوانين الوطنية التي تنظم المساعدة القانونية المتبادلة على أحكام خاصة بالجريمة السيبرانية التي تعكس هذه الحقيقة.[7] وبرغم هذا، فإن بعض الصكوك الثنائية ومتعددة الأطراف، إضافة إلى القوانين الوطنية، تسمح بوسائل الاتصال العاجل، مثل البريد الإلكتروني أو الفاكس أو الأنظمة الإلكترونية،[8] حيث تنص اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية واتفاقية جامعة الدول العربية، على سبيل المثال، أنه "*في الحالات الطارئة*" يجوز للأطراف تقديم طلبات المساعدة المتبادلة عبر وسائل الاتصال العاجل، بما فيها الفاكس أو البريد الإلكتروني، يليها تأكيد رسمي بالوصول.[9] كما تنص الصكوك غير الملزمة على استخدام "*أكثر الوسائل كفاءة، [.....]، بشرط أن استخدام المستويات المناسبة من التوثيق والأمن، وأن يلي الطلب أو الرد تأكيد رسمي بالوصول.*"[10]

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 195 والسؤال رقم 217.

[2] المرجع نفسه.

[3] المرجع نفسه.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 218.

[5] المرجع نفسه.

[6] استبيان دراسة الجريمة السيبرانية. السؤال رقم 141.

[7] استبيان دراسة الجريمة السيبرانية. السؤال رقم 193 والسؤال رقم 216.

[8] المرجع نفسه.

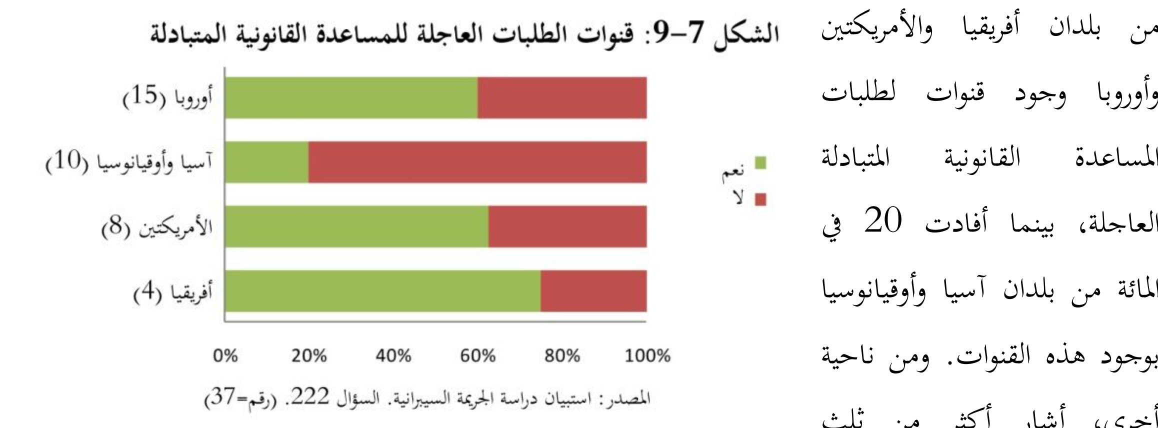
[9] اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، المادة 25(3)، واتفاقية جامعة الدول العربية، المادة 32(3).

[10] مشروع الميثاق النموذجي لدول الكوميسا، المادة 43(ب).

أثناء تجميع المعلومات من أجل هذه الدراسة، أفاد حوالي نصف البلدان المجيبة باستخدام البريد الإلكتروني أو الفاكس من أجل طلبات المساعدة القانونية المتبادلة، بينما أفادت نسبة أصغر بكثير – 5 في المائة – باستخدام النظام الإلكتروني. وعلى النحو المتوقع، عند الأخذ في الاعتبار دور المساعدة القانونية المتبادلة في مرحلة التحقيق، كان استخدام وسائل الاتصال العاجلة أكبر بالنسبة لطلبات المساعدة القانونية مقارنة بطلبات تسليم المجرمين.[1] ووفقا لمتطلبات الصكوك الدولية والإقليمية بشأن الجريمة السيبرانية، أحاطت بلدان عدة أن هذه الاتصالات كانت خاضعة للمتابعة باستخدام البريد والخطابات الدبلوماسية.[2] وقد أفادت إحدى دول أمريكا الجنوبية أنها استخدمت البريد الإلكتروني والفاكس لمتابعة عملية تسليم المجرمين، بينما أشارت البلدان المجيبة من وسط آسيا أنها لم تلجأ إلا للاتصالات الإلكترونية في الحالات عاجلة.[3]

ووفقا لمستويات استخدام البريد الإلكتروني والفاكس والهاتف التي جرت الإفادة بها، أفادت 60 في المائة من بلدان أفريقيا والأمريكتين وأوروبا وجود قنوات لطلبات المساعدة القانونية المتبادلة العاجلة، بينما أفادت 20 في المائة من بلدان آسيا وأوقيانوسيا بوجود هذه القنوات. ومن ناحية أخرى، أشار أكثر من ثلث البلدان المجيبة إلى آليات خاصة للقنوات العاجلة، بما فيها المكاتب المركزية الوطنية للإنتربول، ومجموعة البلدان الثمانية، وشبكات عمل مجلس أوروبا على مدار الساعة.[4] يكون للانضمام لأحد الصكوك الدولية أو الإقليمية التي *تحدد* قنوات المساعدة القانونية المتبادلة أثر معتدل – 55 في المائة من البلدان المجيبة التي لم تكن طرفا في أي صك متعدد الأطراف التي لم تمتلك قنوات للطلبات العاجلة مقارنة بنسبة 40 في المائة من البلدان التي كانت أطرافا في أي صك بشان الجريمة السيبرانية متعدد الأطراف.[5]

الشكل 7–9: قنوات الطلبات العاجلة للمساعدة القانونية المتبادلة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 222. (رقم=37)

ويتجه استخدام الوسائل العاجلة لطلبات المساعدة القانونية بشأن الجريمة السيبرانية بطريقةٍ ما نحو التعامل مع تحديات تأثر الأدلة الإلكترونية. ولكن، لم يفد إلا نصف إجمالي البلدان المجيبة باستخدام هذه

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 197 والسؤال رقم 219.
[2] المرجع نفسه.
[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 222.
[4] المرجع نفسه.
[5] المرجع نفسه.

الآليات. إضافة إلى ذلك، إذا كان زمن الاستجابة للمساعدة الرسمية الواردة خلال الاستبيان بخصوص هذه الدراسة *شاملا* الطلبات التي جرى التعامل معها على أساس "عاجل"، لا يزال متوسط زمن الاستجابة – وبالطبع التوزيع السائد لزمن الاستجابة بالأشهر، وليس بالأيام. وكما هو وارد أدناه، يختلف الموقف فيما يتصل بوسائل التعاون *غير الرسمي*. وبينما يقدم التعاون غير الرسمي مدى محدود من المساعدة، لكن زمن الاستجابة أسرع.

4-7 التعاون الدولي ب - التعاون غير الرسمي

الاستنتاجات الرئيسية:

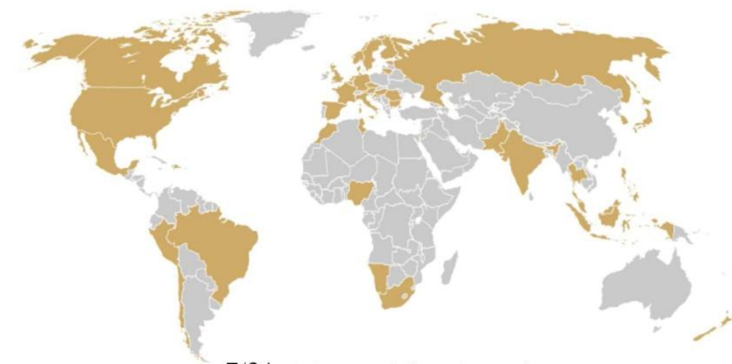
- طرائق التعاون غير الرسمية ممكنة لحوالي ثلثي البلدان المجيبة عن الاستبيان، على الرغم من أن عددا قليلا من البلدان لديها سياسة لاستخدام هذه الآليات
- يوجد عدد من شبكات التعاون غير الرسمية في مجال الجريمة السيبرانية، بما في ذلك مجموعة الثماني ومجلس أوروبا، وشبكات "24-7"
- مبادرات للتعاون غير الرسمي وتسهيل التعاون الرسمي، مثل شبكات "24-7"، والتي تقدم إمكانيات هامة لأوقات استجابة أسرع، تُعدُّ بالأيام
- ومع ذلك، قد تكون هذه المبادرات مستغلّة بشكل غير كاف. يمثل عدد القضايا التي تمت معالجتها بواسطة شبكات "24-7" التي نوّهت إليها البلدان المجيبة عن استبيان الدراسة نحو 3 في المائة من إجمالي عدد قضايا الجريمة السيبرانية التي واجهتها سلطات إنفاذ القانون لهذه المجموعة من البلدان
- تحليل آليات التعاون الرسمي وغير الرسمي غير قادر على استنتاج أن وضع التعاون العالمي الحالي كاف. على الصعيد العالمي، الاختلافات في نطاق أحكام التعاون في أصول المعاهدات متعددة الأطراف والثنائية؛ عدم التزام زمن الاستجابة؛ شبكات إنفاذ القانون غير الرسمية المتعددة؛ والتباين في ضمانات التعاون الذي يمثّل تحديات كبيرة في وجه التعاون الدولي الفعال بشأن الأدلة الإلكترونية في المسائل الجنائية

وجهات النظر الدولية والإقليمية

بالإضافة إلى أشكال التعاون الدولي الرسمية، قد يتم الشروع في خطوات تتعلق بعملية تحقيقات إنفاذ القانون خارج الإقليم من خلال الاتصال غير الرسمي من شرطة إلى شرطة وجهازٍ إلى جهاز. يمكن استخدام هذا الاتصال قبيل طلب المساعدة القانونية المتبادلة الرسمية إلى السلطة المختصة، أو لتسهيل الطلب الرسمي.

تم تصور أساليب التعاون غير الرسمية بالقرار، على وجه الخصوص، من قبل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية واتفاقية جامعة لدول العربية. بينما يمكن توسيط التعاون غير الرسمي من خلال الاتصال المباشر بين شرطة وشرطة، أو من خلال الشبكات الدولية مثل الإنتربول، كل من هذه الوسائل يتطلّب من الدول الأطراف أن تعين "نقطة اتصال متخصصة". تهتم نقطة الاتصال بضمان تقديم المساعدة الفورية في التحقيقات الجنائية المتعلّقة بأنظمة الحاسوب والبيانات أو لجمع الأدلة في الشكل الإلكتروني من الجريمة الجنائية.[1] وبموجب اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، ينبغي أن تسهل النقاط "7/24" من الاتصال، أو، إذا سمحت القوانين والممارسة الوطنية، تنفيذ ما يلي بشكل مباشر: (1) تقديم المشورة التقنية؛ (2) الحفاظ على البيانات؛ و (3) جمع الأدلة وتوفير المعلومات القانونية وتحديد المشتبه فيهم.[2] وعلى نطاقٍ أوسع، تتطلب اتفاقية الجريمة المنظّمة أيضا من الدول الأطراف النظر في الدخول في ترتيبات بخصوص *"التعاون المباشر بين أجهزتهم المعنية بإنفاذ القانون"*.[3]

الشكل 7–10: أعضاء شبكة مجموعة الثماني 7/24 (2007)



المصدر: بيان بروتوكول مجموعة الثماني 7/24

على الصعيد العالمي، يوجد عدد من شبكات التعاون غير الرسمية لمكافحة الجريمة السيبرانية. بالإضافة إلى شبكة 7/24 للدول الأطراف في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية،[4] أنشأت المجموعة الفرعية للدول الثمانية بشأن جرائم التكنولوجيا المتقدمة شبكة 7/24 بهدف تعزيز وتكميل الطرائق التقليدية في الحصول على المساعدات في الحالات التي تنطوي على الاتصالات الشبكية وغيرها من التكنولوجيا ذات الصلة.[5] وكما تظهر الخريطة، فإن عضوية شبكة الدول الثماني تشمل البلدان التي هي طرف في عدد من الاتفاقيات الدولية والإقليمية المختلفة – التي توفر فرصا للتعاون غير الرسمي ووصولا أسرع إلى التعاون الرسمي، وسط البلدان التي قد لا تكون بطريقة أخرى قادرة على الاعتماد على اتفاقيات الجريمة السيبرانية القانونية متعددة الأطراف المشتركة.[6]

---

[1] اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 35؛ اتفاقية جامعة الدول العربية، المادة 43.

2 المرجع نفسه. (اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية).

3 معاهدة الجريمة المنظمة، المادة 27 (2).

[4] نقاط الاتصال 7/24 المحددة في إطار اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، المادة 35 المتوفرة على العنوان التالي:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Document /Internationalcooperation/Res_internatcoop_au thorities_en.asp

[5] مجلس أوروبا، 2008. فاعلية التعاون الدولي ضد الجريمة السيبرانية: أمثلة على الممارسات الجيدة، الصفحة 13.

[6] عضوية شبكة 7/24 للدول الثماني اعتبارا من ديسمبر 2007. أنظر: http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf

"يتم استخدام **التعاون غير الرسمي** [...] 80 في المائة من الوقت، **لأنه أسرع، خاصة مع ما تكشفه التحقيقيات. فليس** هناك **وقت لإهداره** في تقديم طلبات رسمية، والذي يؤدي إلى إحباط التحقيق."

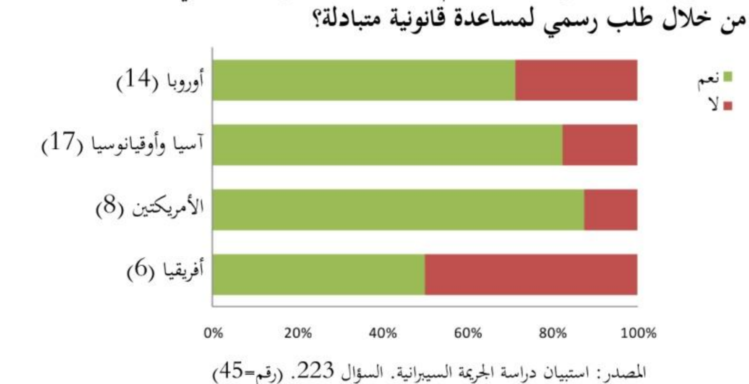
المصدر: استبيان دراسة الجريمة السيبرانية. السؤال رقم 223 (رد من بلد في غربي أفريقيا)

تقدم شبكات 7/24 الميزة العملية للوصول بسهولة لنقطة الانطلاق المعروفة لطلبات التعاون. قد يؤدي تطوّر الشبكات المتعددة، مع ذلك، إلى خطورة الانتقاص من قوة "الاتصال الفردي" للنظام. فخلال جمع المعلومات للدراسة، على سبيل المثال، نوّهت إحدى البلدان إلى أنّ نقطة الاتصال الوطني لشبكة الدول الثماني تقع ضمن مؤسسة إنفاذ القانون، في حين أن نقطة الاتصال الوطنية لشبكة 7/24 المنشاة بموجب اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية تقع ضمن مكتب الإدعاء التابع للمحكمة العليا.[1] كما أن وجود نقاط اتصال متعددة في بلد من شأنه خلقُ تحدٍ للبلدان الأخرى في معرفة أي نقاط المركزية ينبغي التوجه إليها. وقد يؤدي ذلك أيضا إلى تأخير الاستجابة للطلبات عندما تحتاج البلدان المطلوبة للمساعدة للتحقق من صحة أو هوية النقطة المركزية من الآلية التي لم يسبق لها الاتصال معها.

النهج الوطنية نحو التعاون غير الرسمي

أشارت غالبية البلدان المجيبة عن الاستبيان أن المساعدة يمكن تقديمها بشكل غير رسمي، بالإضافة إلى تقديمها من خلال المساعدة القانونية المتبادلة الرسمية.[2] كانت نسبة البلدان القادرة على تقديم المساعدة غير الرسمية أعلى بدرجة ملحوظة في أوروبا وآسيا وأوقيانوسيا والأمريكتين (ما بين 70 و90 في المائة) أكثر مما كانت عليه في أفريقيا (نحو 50 في المائة).[3]

الشكل 7–11: **هل يمكن تقديم المساعدة بشكل غير رسمي، وكذلك من خلال طلب رسمي لمساعدة قانونية متبادلة؟**



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 223. (رقم=45)

كما أشارت الدول التي تعتمد على الاستفادة من التعاون غير الرسمي إلى أن هذه الآليات كانت تعتمد على وجود نظير أجنبي مؤهل ومنظم بشكل جيد. وأوضحت الدول أن هذا كان أكثر احتمالا عندما كان التعاون غير الرسمي في مجال إنفاذ القانون محكوما بشكلٍ من أشكال الاتفاق. نوّه عدد من البلدان أن التعاون غير الرسمي يتم بناء على ذلك وفق الاتفاقيات الإقليمية والثنائية، من خلال استخدام الشبكات التي أنشأتها المنظمات والمؤسسات الدولية والإقليمية؛ وبمساعدة من السفارات والقنصليات وكذلك من خلال الشبكات الخاصة بين

1 رد من خبير إقليمي عينته مجموعة دول أوروبا الغربية ودول أخرى للنتائج الأولية من الدراسة.

2 استبيان دراسة الجريمة السيبرانية. السؤال رقم 223

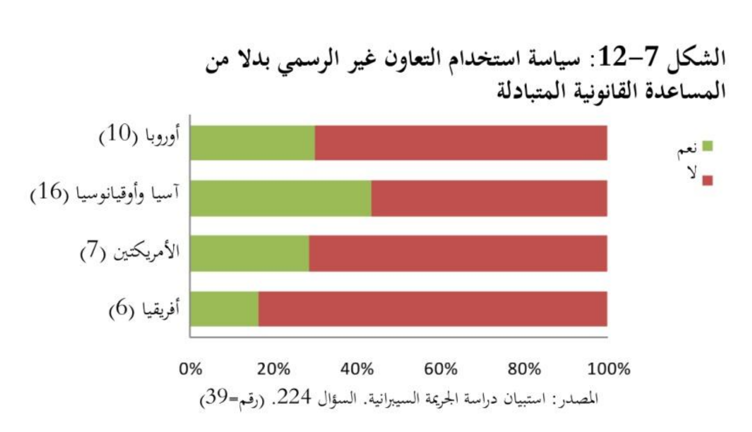
3 المرجع نفسه.

ضباط إنفاذ القانون.[1] في حين أشارت بعض البلدان إلى التعاون المباشر بين الشرطة والشرطة، تحدث آخرون في المقام الأول عن التعاون غير الرسمي من خلال قنوات الإنتربول.[2] وقد نوّه أحد البلدان إلى أن هذا يتفق مع واقع التعاون القانوني الدولي، بقدر وسائل الاتصال غير الرسمية – التي يمكنها أن تكون مع ذلك مفيدة ومرنة – الموجودة في كثير من الأحيان بين الدول التي وضعت علاقات عمل طويلة الأمد.[3] تم تعريف تبادل المعلومات القضائية الدولية من خلال قنوات الشرطة الدولية المعمول بها كخطوة ضرورية للتحقيقات الناجحة.

وعلى الرغم من أن أشكال التعاون غير الرسمي تكون على الأرجح أكثر فعالية عندما تستند إلى اتفاق واضح، أفادت غالبية البلدان أن استخدام التعاون غير الرسمي بدلا من المساعدة القانونية المتبادلة الرسمية لم يكن خاضعا لسياسة محددة.[4] ومع ذلك، سلّط عدد من البلدان الضوء على وجود مبادئ توجيهية وبروتوكولات، بما في ذلك القواعد "غير المكتوبة".

ونوهت أيضا إلى أنه عندما توجد قواعد فإنها يُنصّ عليها في التشريعات الوطنية، مثل المساعدة المتبادلة في أعمال المسائل الإجرامية.[5] وتختلف الممارسة لاسيّما فيما يتعلّق بمن تم تعيينه ليسمح بالمساعدة غير القانونية.

الشكل 7–12: سياسة استخدام التعاون غير الرسمي بدلا من المساعدة القانونية المتبادلة

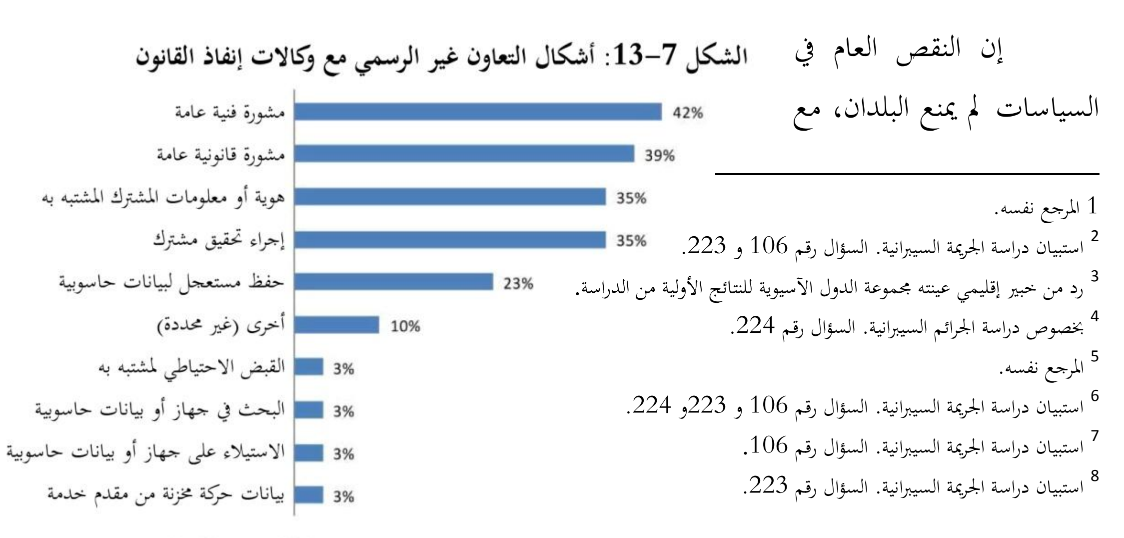


المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 224. (رقم=39)

وتراوحت الخيارات الواردة من المراقب المحلي أو ضابط التحقيق، إلى رئيس قسم الجريمة السيبرانية، إلى حالة المدعي العام أو أية سلطةٍ قضائية، إلى وزارة العدل.[6] كما تميل معظم البلدان للسماح باتخاذ القرارات على مستوى التحقيق – من قبل الشرطة المحلية أو المدعي العام، في بعض الأحيان بالتنسيق مع رؤساء الجهة المختصّين.[7] وقد أشارت إحدى البلدان من جنوب شرق آسيا، على سبيل المثال، إلى أنه في حين مشاركة مكتب المدعي العام طلباتٍ رسمية، فإن مشاركته ليست إلزامية للحصول على المساعدة المقدمة من خلال قنوات التعامل غير الرسمية.[8]

إن النقص العام في السياسات لم يمنع البلدان، مع

الشكل 7–13: أشكال التعاون غير الرسمي مع وكالات إنفاذ القانون



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 106. (رقم=31، 61)

1 المرجع نفسه.

2 استبيان دراسة الجريمة السيبرانية. السؤال رقم 106 و 223.

3 رد من خبير إقليمي عينته مجموعة الدول الآسيوية للنتائج الأولية من الدراسة.

4 بخصوص دراسة الجرائم السيبرانية. السؤال رقم 224.

5 المرجع نفسه.

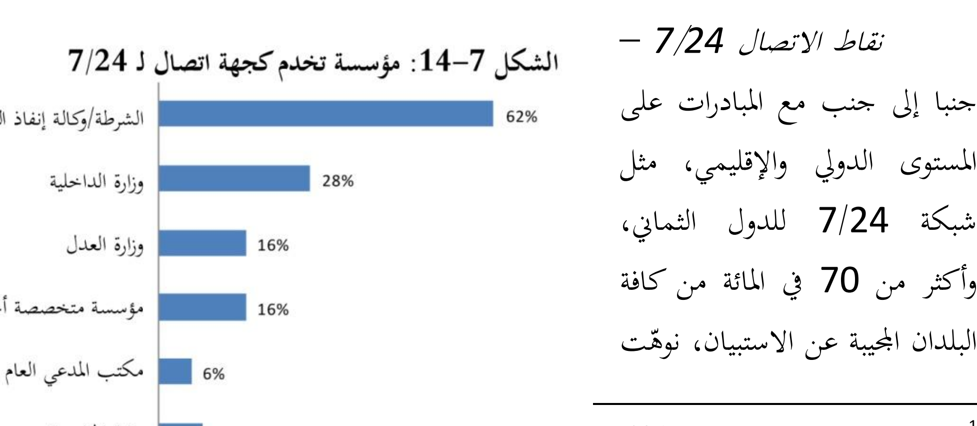
6 استبيان دراسة الجريمة السيبرانية. السؤال رقم 106 و 223و 224.

7 استبيان دراسة الجريمة السيبرانية. السؤال رقم 106.

8 استبيان دراسة الجريمة السيبرانية. السؤال رقم 223.

ذلك، من الإشارة الواضحة لأنواع المساعدة التي يمكن تقديمها من خلال التعاون غير الرسمي – ولكن مع بعض الاختلافات. ذكرت بعض البلدان أن المشورة الفنية والقانونية العامة تتم مبادلتها مع النظائر في جهات إنفاذ القانون الأجنبي تقريبا على بصفة يومية. تتعلّق غالبية هذه المعلومات بالتحقيقات المشتركة أو استخبارات التشغيل العام.[1] كانت كافة البلدان المجيبة عن الاستبيان تقريبا قادرة على توفير هذه المعلومات بشكل غير رسمي، مع 10 في المائة فقط من البلدان مشيرة إلى أن "*كافة الطلبات الرسمية محالة إلى سلطة المساعدة القانونية المتبادلة*".[2] وذهبت بعض البلدان إلى أبعد من ذلك؛ إذ أشارت إلى أن مشاركة بعض البيانات الشخصية (بما في ذلك مالكي أرقام الهاتف وصندوق البريد، والمعلومات من سجلات الفندق، وأصحاب عناوين بروتوكول الإنترنت المتاحة دون تدابير إلزامية)، والحصول على السجلات العامة مثل السجلات الجنائية، وأخذ إفادات الشهود الطوعية، والمراقبة يمكن توفيرها من خلال التعاون المباشر لإنفاذ القانون.[3]

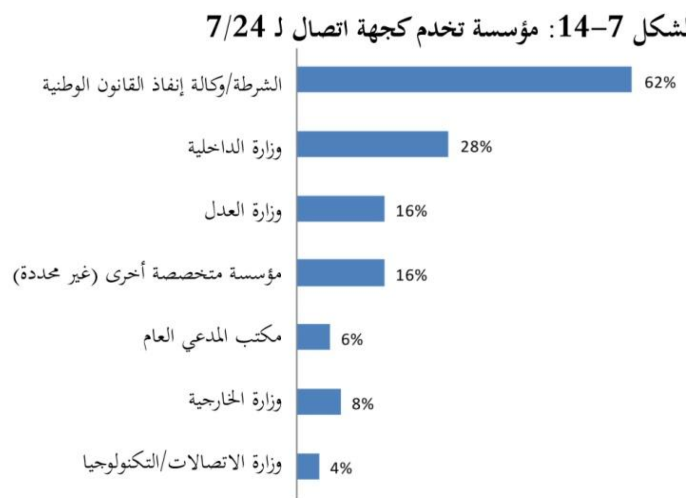
وعموما، فقد تم التنويه إلى أن طلبات تدابير تحقيق محددة مثل الحفاظ المعجل للبيانات والاعتقال المؤقت لأحد المشتبه فيهم أو بحث ومصادرة الأجهزة أو البيانات تتطلب إما تقديم طلب المساعدة القانونية المتبادلة، أو أن يتم متابعة طلب رسمي في غضون فترةٍ زمنيةٍ قصيرة.[4] كما ذكر بلد في أمريكا الشمالية، على سبيل المثال، التعاون بين شرطة وشرطة "*لا يسمح باستخدام أوامر جمع الأدلة أوامر الإلزامية، مثل إصدار مذكرات الاستدعاء أو أوامر الانتاج، وتنفيذ أوامر التفتيش أو غيرها من مذكرات القانون الجنائي*".[5] وأشار بلد واحد فقط إلى أن كافة أنماط المساعدة الرسمية كانت أيضا متاحة من خلال وسائل غير رسمية. كان الوضع المعتاد في غالب الأحيان (بالنسبة لأكثر من ثلثي البلدان المجيبة عن الاستبيان) أن "بعض المساعدة" كان من الممكن تقديمها بشكلٍ غير رسمي.[6] يتناسب هذا مع النتيجة أن غالبية الدول تعتمد على الوسائل الرسمية للحصول على الدلائل خارج الإقليم في تحقيقات الجريمة السيبرانية.[7]



نقاط الاتصال 7/24 –

جنبا إلى جنب مع المبادرات على المستوى الدولي والإقليمي، مثل شبكة 7/24 للدول الثماني، وأكثر من 70 في المائة من كافة البلدان المجيبة عن الاستبيان، نوهّت

الشكل 7–14: مؤسسة تخدم كجهة اتصال لـ 7/24



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 107. (رقم=50، 70)

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 106

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 223.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 106.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 106و 223.

5 نفس المرجع (السؤال 223).

[6] نفس المرجع (السؤال 223).

[7] استبيان دراسة الجريمة السيبرانية. السؤال رقم 105.

إلى وجود مؤسسة خادمة مثل نقطة الاتصال 7/24.[1] ومن المرجح، مع ذلك، أن تبالغ هذه النسبة بشكل ملحوظٍ في الدرجة التي تتواجد فيها نقاط الاتصال 7/24 على مستوى العالم – في ضوء الامتداد الحالي لشبكات 7/24 الدولية والإقليمية وعدد قليل نسبيا من البلاد المجيبة عن الاستبيان من مناطق مثل أفريقيا. إضافة إلى ذلك، سلط عدد من البلدان المجيبة عن الاستبيان الضوءَ على أهمية شبكات 7/24. كما صرّح أحد البلدان، على سبيل المثال، بأنه "من الضروري امتلاك نقطة مركزية (مكتب المقر رئيسي) للوصول إلى قائمة اتصال الإنتربول 7/24 بالإضافة إلى نقاط طوارئ الاتصال 7/24 للدول الثماني".[2] وعلى نحوٍ أكثر شيوعا فإن نقاط الاتصال 7/24 تم الاعتراف بها في الشرطة الوطنية وجهات إنفاذ القانون، تليها وزارات الداخلية ووزارات العدل.[3] وكما هو ملاحظ أعلاه، فإن نقاط الاتصال 7/24 تستطيع على حدس سواء أن تيسر، وإذا أذن لها، أن تتصرف بشكل مباشر، سواء فيما يتعلّق بالتعاون الرسمي وغير الرسمي. ربما يكون من غير المتوقع أنه قد تم التنويه إلى أن معظم الطلبات شيوعا تم استلامها من قبل نقاط اتصال 7/24 بخصوص هوية المشترك أو معلوماته، تليها طلبات الحفاظ المعجّل وتوريد بيانات المرور المخزنة.[4] هذا في تماشٍ مع المهام المتصوّرة لنقاط اتصال 7/24 من خلال معاهدة مجلس أوروبا، على سبيل المثال.[5]

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 107.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 99.

3 نفس المرجع

4 نفس المرجع

5 اتفاقية مجلس أوروبا، المادة 35

وفيما يتعلق بأكثر أنماط الجريمةٍ شيوعا نوّهت البلدان المجيبة عن الاستبيان إلى أن طلبات المساعدة تهتمّ في الغالب بالمنتجات ذات الصلة بالحاسوب، وتوزيع أو حيازة المواد الإباحية عن الأطفال بالإضافة إلى مراودة و"استمالة" الأطفال. يعقب ذلك الطلبات المتعلقة بالاحتيال أو التزوير المتعلق بالحاسوب.[1] ترتفع نسبة القضايا المتعلقة باستغلال الأطفال في المواد الإباحية، التي اطلعت عليها النقاط المحورية 7/24، إلى حدٍ ما عن كافة الجرائم السيبرية التي تعاملت معها سلطات إنفاذ القانون بشكلٍ عام.[2] قد يعكس ذلك درجة عالية من الإنفاق العابر للحدود من الضحايا والجناة في هذه الجريمة. وفي المقابل نوّه بلد في أمريكا الجنوبية إلى أن النقطة المحورية 7/24 الخاصة به تتعامل بشكل متكرر مع الجرائم المتعلقة بالهجمات على الأنظمة الحكومية والتشويش على المواقع وهجمات الروبوت والتصيد الاحتيالي.[3]

مثال لتشريع محددة بشأن الجريمة السيبرانية في شبكات 7/24 من بلد في غرب أفريقيا

تعيين نقطة الاتصال لشبكة 7/24

(1) من أجل تقديم المساعدة العاجلة لغرض التعاون الدولي بموجب هذا القانون، يتعين على مستشار الأمن القومي تعيين نقطة الاتصال التي ستكون متاحة على مدار الأربع والعشرين ساعة في اليوم ولمدة سبعة أيامٍ في الأسبوع، والحفاظ عليها.

(2) يمكن توصيل نقطة الاتصال هذه بنقاط الاتصال الأخرى وفقا للاتفاقات والمعاهدات أو الاتفاقيات التي تلتزم بها [هذه الدولة]، أو تنفيذا لبروتوكولات التعاون مع الجهات الدولية لإنفاذ القانون أو القضاء.

(3) تحتوي المساعدة الفورية التي ستقدمها نقطة الاتصال على:

أ) تقديم المشورة الفنية إلى نقاط الاتصال الأخرى.

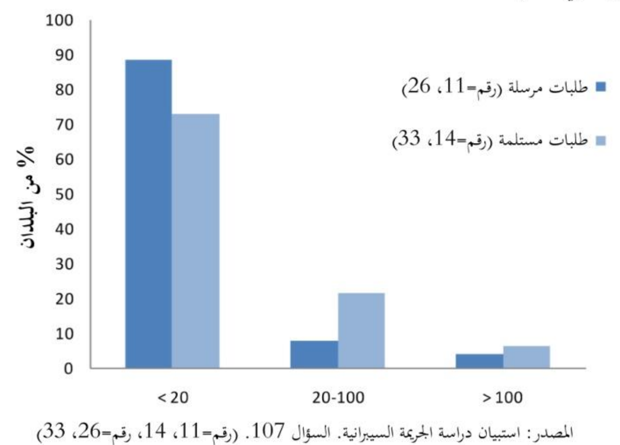
ب) الحفاظ عل البيانات على وجه السرعة في حالات الطوارئ أو الخطر.

ج) جمع الأدلة التي تمتلكها السلطة القانونية في حالات الطوارئ أو الخطر في التأخير.

د) الكشف عن المشتبه بهم وتوفير المعلومات لقانونية في حالات الطوارئ أو الخطر في التأخير.

هـ) الإرسال الفوري للطلبات بشأن التدابير المشار إليها في ... هذا القسم بغية التنفيذ المستعجل لها.

الشكل 7–15: عدد الطلبات المرسلة والمستلمة من قبل نقاط الاتصال المركزية في العام



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 107. (رقم=11، 14، رقم=26، 33)

كان عدد قليل من البلدان فقط (على الرغم من التوزيع الجغرافي الواسع للغاية) قادرا على توفير الإحصاءات المتعلقة بعدد الطلبات لمرسلة والمستلمة من قبل نقاط الاتصال

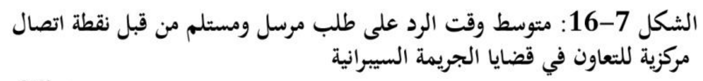
1 استبيان دراسة الجريمة السيبرانية. السؤال رقم 107.

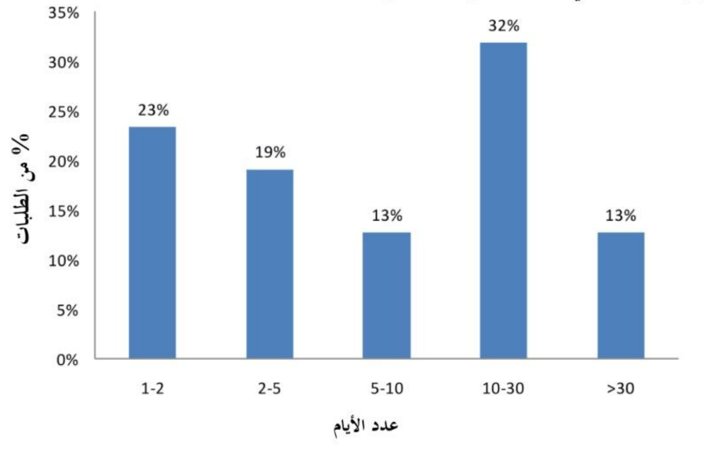
2 أنظر لفصل الثاني (الصورة العالمية)، القسم 2.2 صورة الجريمة السيبرانية العالمية، توزيع أعمال الجريمة السيبرانية.

3 استبيان دراسة الجريمة السيبرانية. السؤال رقم 107.

7/24 في كل عام. تظهر البيانات المنوّه إليها من خلال استبيان الدراسة أن أكثر من 70 في المائة من البلدان تعاملت مع أقل من 20 طلبا (تم إرساله أو استلامه) من خلال نقطة الاتصال 7/24 سنويا. وتعاملت بلدان فقط من البلدان المجيبة عن الاستبيان مع أكثر من 100 طلب سنويا.[1]

وعلى سبيل المقارنة، فقد أبلغت سلطات إنفاذ القانون في هذه البلدان متوسط ما يقرب من 1000 حالة جريمة سيبرانية سنويّا.[2] وعموما، فإن العدد الإجمالي لطلبات 7/24 الذي ذكر سنويا لهذه المجموعة من البلدان يمثل 3 في المائة من العدد الإجمالي لحالات الجريمة السيبرانية التي واجهها المكلفون بإنفاذ القانون في سنة.[3] وبأي حال من الأحوال فإن كافة الجرائم السيبرانية التي تنموا إلى علم إنفاذ القانون تتطلب اشتراك شبكة 7/24 – يمكن التحقيق في كثير من القضايا بنجاحٍ على المستوى الوطني وحده. إضافة إلى ذلك، نوّهت مجموعة من البلدان التي قدّمت بيانات عن استخدام نقاط اتصال 7/24 إلى أن 60 في المائة من القضايا، في المتوسط، تشمل بعدا عبر الحدود.[4] وعلى هذا النحو، قد يكون هناك مجال كبير لتوسيع استخدام الآلية.


الشكل 7–16: متوسط وقت الرد على طلب مرسل ومستلم من قبل نقطة اتصال مركزية للتعاون في قضايا الجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 107. (رقم=25، 47)

يجازف القصور في استخدام شبكات 7/24 بفقدان المكاسب المحتملة في وقت الاستجابة للطلب. نوّهت البلدان المجيبة عن استبان الدراسة إلى أن ما يقرب من 90 في المائة من الطلبات التي تمت معالجتها بواسطة نقاط الاتصال 7/24 تلقت ردا في غضون شهر واحد.[5] تلقت أكثر من 20 في المائة من الطلبات ردا في غضون يوم إلى يومين. يمكن توقع وقت استجابة أسرع لطلبات 7/24 من طلبات المساعدة القانونية المتبادلة، ليس فقط بسبب بطبيعة نظام 7/24 ولكن أيضا يرجع ذلك إلى حقيقة أن –كشكل من أشكال التعاون غير الرسمي– مجموعة الإجراءات التي يمكن أن تقوم بها نقطة اتصال 7/24 أكثر محدودية من إجراءات تقديم المساعدة القانونية المتبادلة الرسمية.

---

1 نفس المرجع

2 استبيان دراسة الجريمة السيبرانية. السؤال رقم 54-71.

3 حسب يستند إلى استبيان دراسة الجريمة السيبرانية. السؤال رقم 107 و 54-71 لكافة البلدان المجيبة عن مجموعتي الأسئلة.

4 استبيان دراسة الجريمة السيبرانية. السؤال رقم 83. بيانات فقط للبلدان المجيبة عن السؤال رقم 107.

5 استبيان دراسة الجريمة السيبرانية. السؤال رقم 107.

على هذا النحو، يتوافق "وقت الاستجابة" المدروس مع مجموعة مختلفة من إجراءات المساعدة أكثر من تلك التي تم عرضها من خلال تقديم المساعدة القانونية المتبادلة – وكلا شكلي "وقت الاستجابة" لا يمكن مقارنتهما مباشرة. وكما ذكرنا آنفا، فإن آلية غير رسمية، مثل نقطة الاتصال 7/24، تكون أكثر عرضة لتقديم المشورة الفنية والقانونية العامة وتسهيل الإجراءات الأكثر رسمية أكثر من القيام بإجراءات جمع الأدلة نفسها.[1] إضافة إلى ذلك، فإن الحقيقة أن نقاط الاتصال 7/24 تقدّم الرد في كثيرٍ من الأحيان في غضون أيامٍ يمثل بداية هامة لقنوات الاتصال لتسهيل التعاون في الوقت المناسب، بما في ذلك – ربما – الإجراءات التي تتطلب طلبا أكثر رسمية.

تعاون كاف؟

توصّل هذا الفصل مبكرا إلى أن القواعد الحالية للولاية القضائية كافية، على الراجح، لتجنب الثغرات القضائية في التحقيقات ومكافحة أعمال الجريمة السيبرانية. ويعد تحليل آليات التعاون الرسمي وغير الرسمي، من ناحية أخرى، غير قادرٍ على التوصّل إلى أن الوضع العالمي الحالي يكفي لتلبية تحقيقات الجريمة السيبرانية وتحديات الإدعاء العام.

في حين أن عددا من الخيارات الموجودة – بما في ذلك استخدام التعاون غير الرسمي، إما مباشرة أو لتسهيل التعاون الرسمي– إلا أن 70 في المائة من البلدان نوّهت في معظم الأحيان إلى استخدام طلبات المساعدة القانونية المتبادلة الرسمية للحصول على الأدلة الإلكترونية التي تقع في ولاية قضائية أخرى. ومن ضمن المساعدة القانونية المتبادلة الرسمية، الأدوات الثنائية التي تهيمن – بالاعتماد على وسائل الاتصال التقليدية مثل البريد والرسائل الدبلوماسية والناتجة في متوسط أوقات استجابة في ترتيب الأشهر بدلا من الأيام. وكما ذكرت الدول من قبل فإن أوقات استجابة التعاون الطويلة تخلق تحدياتٍ كبيرة بسبب تقلّب الأدلة الإلكترونية.

بينما تنخرط العديد من البلدان في التعاون غير الرسمي في مجابهة قضايا الجريمة السيبرانية في نطاق زمني أسرع، تختلف مجموعة إجراءات التحقيقات التي يمكن تقديمها بشكل كبير، فضلا عن وجود أو عدم وجود سياسات واضحة في استخداماتها. وتعترف العديد من البلدان بأن الأدلة التي تم الحصول عليها من خلال التعاون غير الرسمي لا يمكن اعتبارها إمداد مستداما للأدلة في المحاكمة. وربما يكون بسبب تنوع النهج، قد يعتبر حتى التعاون غير الرسمي في بعض الحالات آلية مرهقة.[2] بينما تبرمُ شبكات 7/24 وعدا لتبسيط التعاون غير الرسمي وتسهيل التعاون الرسمي، فإنها تميل إلى أن تُستخدم بشكل نسبي في النادر عند مقارنتها بالتجمع المحتمل لحالات الجريمة السيبرانية العابرة للحدود التي تنموا إلى علم سلطات إنفاذ القانون.

---

1 أنظر أعلاه، القسم 7–4 التعاون الدولي 2 – التعاون غير الرسمي والنهج الوطنية إلى التعاون غير الرسمي.

2 رد من خبير إقليمي عينته مجموعة دول أوروبا الغربية ودول أخرى للنتائج الأولية من الدراسة.

تنشأ الكثير من هذه التحديات من اختلاف عضوية الصكوك الدولية والإقليمية. يمكن ملاحظة ذلك في مجالات مثل الاختلافات في توافر قنوات المساعدة القانونية المتبادلة العاجلة، والقدرة على تقديم التدابير المتخصصة، مثل التحفظ على البيانات، وذلك في استجابة لطلبات التعاون. تجازف صورة التعاون الدولي الحالي بظهور تكتلات البلاد التي لديها الصلاحيات والإجراءات اللازمة للتعاون فيما بينها، ولكنها مقيدة، بالنسبة لكافة البلدان الأخرى، إلى الأشكال "التقليدية" من التعاون الدولي الذي لا يراعي خصوصيات الأدلة الإلكترونية. وهذا هو الحال في التعاون في إجراءات التحقيق بشكل خاص. ويعني عدم وجود نهج مشترك، بما في ذلك ضمن صكوك الجريمة السيبرانية الحالية متعددة الأطراف، أن طلبات الإجراءات، مثل التحفظ المعجّل على البيانات خارج تلك البلدان مع الالتزامات الدولية لضمان مثل هذا التسهيل وجعله متاحا عند الطلب، قد لا يتم الوفاء به بسهولة. إن إدراج هذه السلطة في صياغة اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني قد يتجه صوب إغلاق هذه الثغرة. وعلى الصعيد العالمي، فإن الاختلافات في نطاق أحكام التعاون في الصكوك متعددة الأطراف والثنائية؛ وعدم الالتزام بوقت الاستجابة؛ وشبكات إنفاذ القانون غير الرسمية المتعددة؛ والتباين في ضمانات التعاون تمثل تحديات كبيرة تؤثر على التعاون الدولي الفعال بشان الأدلة الإلكترونية في المسائل الجنائية.

5-7 الأدلة خارج الإقليم من السحابية ومقدمي الخدمات

الاستنتاجات الرئيسية:

- أصبحت إمكانية تحديد موقع البيانات زائفة على نحو متزايد، رغم إمكانية معرفتها من الناحية الفنية، وذلك بسبب التطورات في مجال الحوسبة السحابية، إلى حد أن طلبات المساعدة القانونية التقليدية المتبادلة غالبا ما تكون موجّهة إلى البلد الذي يتواجد فيه مقر مزود الخدمة بدلا من البلد الذي توجد فيه البيانات فعليا
- من خلال استخدام الاتصال المباشر من جهاز المشتبه فيه أو من خلال استخدام بيانات اعتماد الوصول، أو من خلال وصول المحققين على نحو متزايد – بقصد أو بدون قصد – إلى البياناتِ خارج الحدود خلال جمع الأدلةِ دون الحصول على إذنٍ من البلدِ الذي توجد فيه البيانات ماديا
- قد يحصل المحققون في بعض الأحيان على البيانات من مقدمي الخدمة خارج الإقليم من خلال الطلبات المباشرة غير الرسمية على الرغم من أن مقدمي الخدمة في الغالب يطلبون الإجراءات القانونية الواجبة
- لا تغطي الأحكام القائمة ذات الصلة بشأن الوصول "عبر الحدود" المنصوص عليها في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية واتفاقية جامعة الدول العربية المتعلّقة بجرائم تكنولوجيا المعلومات مثل هذه الحالات بشكلٍ كافٍ بسبب التركيز على الحصول على "موافقة" الشخص صاحب السلطة القانونية للكشف عن البيانات، والمعرفة المفترضة لمكان البيانات في وقت الوصول أو الاستلام
- تتطلّب هذه التحديات ما يلي: (1) إعادة صياغة مفهوم إلى أيّ مدى يمكن استخدام "موقع البيانات" كقاعدةٍ توجيهيةٍ. (2) تطوّر المعايير المشتركة والضّمانات المتعلّقة بالملابسات، إن وجدت، التي بموجبها قد يتم الوصول المباشر إلى البيانات خارج الحدود من قبل المكلّفين بإنفاذ القانون

التحدي

كما أوضح هذا الفصل، فإن النهج الحالية للتعاون الدولي في قضايا الجريمة السيبرانية تواجه تحدّيات كبيرة – بما في ذلك فترات الاستجابة الطويلة للحصول على المساعدة القانونية المتبادلة، وعدم تماثل سلطات التحقيق الوطنية في الحصول على بيانات الحاسوب كدليل. أما التحدّي الثالث – والذي تم التلميح إليه في القسم المتعلّق بالسلطة القضائية ولكن لم يتم تفصيله – فيكمن في تحديد الولاية القضائية ذات الصلة التي ينبغي توجيه طلب التعاون إليها في المقام الأول للحصول على الأدلة الإلكترونية. يصبح هذا التحدّي متزايد الحدة حال انتقال خدمات الحاسوب إلى خوادم ومراكز بيانات موزّعةٍ جغرافيا، والتي تعرف باسم الحوسبة السحابية.

اتسمت خدمات الحوسبة السحابية بأنها "بنية تحتية كخدمة" و "برمجيّات كخدمة" و "ونظام أساسي كخدمة" تغطّي توفير الأجهزة "الافتراضية" على الإنترنت ونظام الخادم ونظام التشغيل والتخزين على التوالي.[1] في هذا السياق تكون "السحابية" مصطلحا جديدا لفكرة قديمة – تسخّر البنية التحتية وخبرات منظّمة أخرى لتقديم موارد حوسبيةٍ كخدمة عبر الإنترنت. أما الأجهزة الفيزيائية وراء الخدمات السحابية الموجودة في مراكز البيانات الموجودة في نقاط استراتيجية تهدف إلى تقليل التأخير في تقديم الخدمات بالإضافة إلى تكاليف الكهرباء وأجهزة التبريد. قد يستطيع مستخدمو جوجل، على سبيل، من الوصول إلى البيانات المخزّنة أو المعالجة في أمريكا الشمالية وجنوب شرق آسيا وشمال أو غرب أوروبا.[2]

يسود زعم فحواه أنه لا يمكن معرفة مكان تخزين البيانات في السحابية، وأنه من الممكن أن تكون البيانات مجزّأة عبر مواقع متعددة. ومن المؤكّد الصحيح أن قواعد البيانات يمكن استضافتها عبر مراكز بيانات متعددة، توجد في بلدانٍ مختلفة، وتحتوي على نسخٍ متعددةٍ من نفس البيانات.[3] قد يشمل هذا وضع بيانات حيوية آليّا عبر مراكز البيانات الموجودة فعليّا في بلدان مختلفة.[4] ومن الصحيح أيضا أنّ الاتفاقات التعاقدية بين مقدّمي الخدمات السحابية والمستخدمين لا تكشف دائما موقع مركز البيانات أو تحتوي على بيانات أو شروط متعلقة بالموقع الجغرافي الذي ستستلم فيه البيات.[5] ومن ناحية أخرى، فإن بعض مقدّمي السحابية يمكنون المستخدمين من تعيين المنطقة الفعلية التي ستوجد فيها الخدمات والخوادم الخاصة بهم، ويتعهدوا بعدم نقل المحتوى من المنطقة المحددة دون إخطار العملاء.[6] بالإضافة إلى ذلك، فإن بروتوكولات الأدلة الجغرافية أيضا قيد التطوير للتحديد البعيد لمنشأ مصدر البيانات – تمكين التحقيق المستقل للموقع الجغرافي للبيانات في السحابية.[7] وعموما، فإن تزايد متطلّبات التوافق، ومتطلّبات العملاء، وتكنولوجيا إدارة البيانات تتجه نحو موقع بيانات سحابية دقيق.

---

1 أنظر، على سبيل المثال، المديرية العامة في البرلمان الأوروبي للسياسات الداخلية وحقوق المواطنين والشؤون الدستورية 2012. مكافحة الجريمة السيبرانية وحماية الخصوصية في السحابة.

2 أنظر http://www.google.com/about/datacenters/inside/locations/index.html

3 أنظر، على سبيل المثال، http://www.datastax.com/wp-content/uploads/2012/09/WP-DataStax-MultiDC.pdf في إشارة إلى استخدام التحكم في عمليات مركز البيانات المتعددة عبر "عدة مناطق جغرافية" من قبل eBay و Netflix من بين غيرها.

4 أنظر، على سبيل المثال،

Peterson, Z.N.J., Gondree, M., Beverly, R., 2011. A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud.

وكمثال لتكنولوجيا التنسيب الآلي عبر مراكز البيانات الموزعة جغرافيا، أُنظر

Agarwal, S., et al., 2010. Volley: Automated Data Placement for Geo-Distributed Cloud Services.

5 Benson, K., Dowsley, R., Shacham, H., 2011. Do you know where your cloud files are? Proceedings of the 3rd ACM Workshop on Cloud Computing Security, pp.73-82.

6 أنظر، على سبيل المثال، Amazon Web Services, 2012. Risk and Compliance. November 2012 متاح على:
http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

7 المرجع نفسه. عرض التحديد الناجح للمواقع الجغرافية التقريبية للبيانات في سحابة الأمازون. أنظر أيضا، Albeshri, A., Boyd, C. and Gonzalez Nieto, J., 2012. الأدلة الجغرافية: أدلة المواقع الجغرافية لبيئة الحوسبة السحابية. أعمال المؤتمر الدولي 32 لورش عمل نظم الحوسبة الموزعة 2012. جمعية مهندسي الكهرباء والإلكترونيات (IEEE) في ماكاو والصين من الصفحة 506-504.

ومع ذلك، فإن القضية تظل – حتى عند تحديد البيانات السحابية – تكشف عن نمطٍ من البيانات المتناثرة، والعابرة في بعض الأحيان، والبيانات، بما في ذلك النسخ في سلطات قضائية متعددة. وعندما تعتبر البيانات السحابية دليلا في تحقيقات الجريمة السيبرانية قد تكون أيضا "خارج الحدود" (في بلدان متعددة) فيما يتعلّق بالبلد المحقق. وفي كثير من الحالات، وحتى الحقيقة الأساسية أن الاختصاص القضائي الخارجي قد لا يكون معروفا على وجه اليقين من قبل المحققين المكلّفين بإنفاذ القانون.[1] تعد نقطة البداية، في كثير من الأحيان، مجرد اسم مزود الخدمة السحابية – مثل الأمازون أو جوجل. وفي حين وجود الإمكانية التقنية يكون من غير المحتمل مقدرة محقق إنفاذ القانون – في بداية التحقيق – على معرفة البلد الذي تقع فيه البيانات السحابية بشكل فعلي (حتى لو تم إثبات عدم نقلها بالفعل). وإذا كان البلد المحقق ليس مقر مزود الخدمة السحابية فإن أسلوب المساعدة القانونية المتبادل "التقليدي" قد يتطلّب بلاغا إلى السلطة المركزية المختصّة بالسلطة القضائية الوطنية لمزود السحابة، مع طلب الحفظ أو إنتاج البيانات الحاسوبية أو كليهما معا.

ومن الجدير بالذكر أنه في إطار هذا الأسلوب قد لا يتم حتى إرسال طلب المساعدة القانونية المتبادلة إلى البلد *الذي تتواجد فيه البيانات فعليا*. فموقع التواصل الاجتماعي الفيس بوك، على سبيل المثال، يستضيف بيانات العديد من المستخدمين في مركز بيانات في بلد واحد أوروبا الشمالية،[2] ولكنه يحدد أنه يفصح عن السجلّات وفقا للقوانين المعمول بها والمقتبسة من بلد في أمريكا الشمالية.[3] أما بالنسبة لإنفاذ القانون الأجنبي، فإن المبادئ التوجيهية لفيس بوك تشير إلى أن طلب المساعدة القانونية المتبادلة أو الإنابة القضائية الموجّهة إلى بلدٍ في أمريكا الشمالية قد يتطلّب فرض الكشف عن محتويات حساب الفيس بوك.[4] وفي الواقع فإن مصالح الدولة التي يتم فيها تخزين البيانات السحابية تفقد أهميتها بالنسبة لمصلحة الدولة التي يتم على أراضيها "التحكم" في البيانات.[5]

سلطت البلدان الضوء على هذه التحديات خلال جمع المعلومات للدراسة. وعندما تم السؤال، على سبيل المثال، عن كيفية الحصول على الأدلة الإلكترونية من مقدمي الخدمة الخاضعين لسلطة قضائية أخرى، علّق عدد من البلدان بأن عملية الحصول على البيانات من خارج الإقليم عمليّة مطوّلة مصحوبة بصعوباتٍ في تحديد *"السلطات الأجنبية مع كلٍ من السلطات القانونية والخبرة التقنية في الأماكن التي تقع فيها الأدلة الرقمية ماديا."*[6]

---

1 على الرغم من أنه ربما قد يفترض بناء على معرفة واسعة بمواقع مقدّم الخدمة السحابية ومركز البيانات.

2 أنظر https://www.facebook.com/luleaDataCenter

3 أنظر /http://www.facebook.com/safety/groups/law/guidelines

4 المرجع نفسه

5 Sieber, U., 2012. Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag. Munich: C.H. Beck.

6 استبيان دراسة الجريمة السيبرانية. السؤال رقم 105.

النهج الدولية والإقليمية

إن تحديات الحصول على البيانات من خارج الإقليم والتي تسيطر عليها أطراف أخرى شيء تم الاعتراف به منذ زمن. فأثناء صياغة اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، على سبيل المثال، تم تضمين المادة 32(ب) بهدف تمكين الأطراف، دون الحصول على إذن من طرف آخر، من: (أ) إتاحة الوصول علانية (مصدر مفتوح) إلى البيانات المخزنة بغض النظر عن موقع وجود البيانات جغرافيا. (ب) الوصول إلى أو استلام، من خلال نظام الحاسوب في أراضيها، بيانات الحاسوب المخزّنة الواقعة في طرف آخر، إذا حصل الطرف على الموافقة القانونية والاختيارية من الشخص الذي لديه السلطة القانونية للإفصاح عن البيانات للطرف من خلال نظام الحاسوب ذلك.[1] ومنذ ذلك الحين تم تضمّين مادةٍ بشروطٍ مطابقة تقريبا في اتفاقية جامعة الدول العربية.[2]

ولأن الأمر يتعلّق بشكل خاصٍ بالحصول على البيانات من خارج الإقليم في تحقيقات إنفاذ القانون، فإن هذه المناقشة تركّز على الإجراءات الواردة في المادة 32(ب) من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية (الوصول إلى البيانات المخزّنة مع الموافقة). تسمى مثل هذه الإجراءات بشكل عام الوصول "عبر الحدود".

تمت صياغة المادة 32(ب) بشروط متساهلة، بقدر ما تصوّر أن الدول الأطراف في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية *قد* تشرع في مثل هذه الإجراءات. إنها لا تحظر بشكل مباشر على الدول الأطراف منع الدول الأطراف الأخرى من الوصول إلى البيانات المخزّنة في أراضيها – ولكن إن قام بلد طرف بفعل ذلك فإن هذا ما يمكن اعتباره متنافيا مع روح المادة. فالوصول "*دون إذن*" من بلدٍ طرف آخر يتم تفسيره على أنه "*الوصول من طرفٍ واحد إلى بيانات الحاسوب المخزّنة في طرفٍ آخر دون البحث عن المساعدة المتبادلة*"[3] كما تغض المادة الطرف عن نقطة إشعار الطرف الآخر – لا تحظر ذلك ولا تتطلّبه. وتجدر الإشارة أيضا إلى أن المادة 32(ب) تهتم بالوصول إلى بيانات الحاسوب المخزنة أو استلامها بشكل عام، وليست مقصورة على سياق التحقيقات في الجريمة السيبرانية. المنظور الأول هو أن المادة 32(ب) تشكّل قاعدة تسمح بشكل صحيح بممارسة سلطة الدولة على أراضي دولة أخرى ضمن الاستثناءات التي نصّ عليها القانون الدولي.[4] أما المنظور الآخر فهو أن هذا الوصول يتنافى مع مبدأ السيادة وعدم التدخل إذا تم تنفيذه دون موافقة الدولة التي تيتم تخزين البيانات في إقليمها.[5] وأما المنظور الثالث فهو أن مثل هذه الأعمال لا تمثّل الحد الأدنى من "التدخل" في الشؤون الداخلية أو الخارجية للدولة التي تيتم تخزين البيانات في إقليمها.[1]

---

1 أنظر، اتفاقية مجلس أوروبا بشأن الجرائم السيبرانية، المادة 32.

2 أنظر، اتفاقية جامعة الدول العربية، المادة 40.

3 مجلس أوروبا، لجنة إتفاقية الجريمة السيبرانية (T-CY)، المجموعة الفرعية المخصصة في الولاية القضائية والوصول إلى البيانات عبر الحدود 2012. الوصول عبر الحدود والولاية القضائية: ما هي الخيارات؟ T-CY (2012) 3-6 ديسمبر، الصفحة 21.

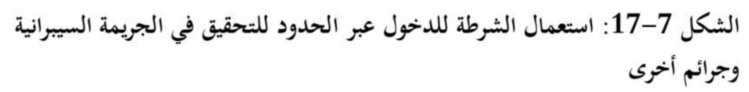
.4 المرجع نفسه، في الصفحة 27، نقلا عن "قاعدة محررة مستمدة من العرف والمعاهدة الدوليه" كما وردت في قضية لوتس السلسلة PCIJ السلسلة A رقم 10 في 18 (1927).

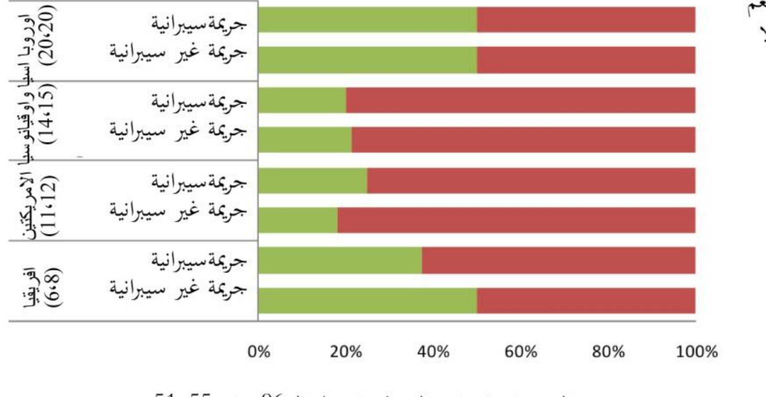
5 Sieber, U., 2012. *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag*. Munich: C.H. Beck.

لم تكن الحوسبة السحابية متطوّرة بالتأكيد في وقت صياغة المادة 32(ب) من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية. ومع ذلك، فإن واضعي الصياغة تصوروا على وجه التحديد تطبيق المادة 32(ب)، من بين أمور أخرى، إلى الحالة التي *"قد يكون فيها البريد الإليكتروني الخاص بالشخص مخزّنا في بلدٍ آخر من قبل مزود الخدمة"*.[2] على هذا النحو، من الممكن أن تطبّق المادة 32(ب) في نطاقٍ واسع من الظروف، بما في ذلك الوصول أو استلام بيانات الحاسب من أفراد خارج الإقليم؛ ومنظمات القطاع الخاص؛ ومقدمي الخدمة؛ وفي عالم اليوم – مشغلي الخدمة السحابية. هناك ميزة محتملة للمادة 32(ب) لإنفاذ القانون وهي أنه إذا وردت موافقة قانونية واختيارية فلا يتوجب على المحققين اتباع إجراءات المساعدة القانونية المتبادلة التي تتحرك ببطء شديد لالتقاط البيانات العابرة.

الممارسة الوطنية

تم سؤال البلدان، خلال جمع المعلومات للدراسة، عن استخدام "الوصول عبر الحدود إلى نظام الحاسوب أو البيانات" كإجراء تحقيقي،[3] وعما إذا كان من المسموح به "الوصول عبر الحدود" إلى نظام الحاسوب أو البيانات في داخل البلد من خلال إنفاذِ قانون أجنبي.[4]


الشكل 7–17: استعمال الشرطة للدخول عبر الحدود للتحقيق في الجريمة السيبرانية وجرائم أخرى



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 96. (رقم=55، 51)

وفيما يتعلّق باستخدام الوصول "عبر الحدود" من قبل سلطات إنفاذ القانون، نوّه نحو 20 في المائة من البلدان في الأمريكتين وآسيا وأوقيانوسيا إلى أن هذا الإجراء قد تم استخدامه، إما من أجل التحقيقات في الجريمة السيبرانية أو غيرها من الجرائم. ارتفع ذلك إلى نسبة 40 في المائة

---

1 مجلس أوروبا، لجنة إتفاقية الجريمة السيبرانية (T-CY)، المجموعة الفرعية المخصصة في الولاية القضائية والوصول إلى البيانات عبر الحدود 2012. الوصول عبر الحدود والولاية القضائية: ما هي الخيارات؟ T-CY (2013) 3-6 ديسمبر، الصفحة 27.

فيما يتعلّق باعتراض المواقع السلبية في بلدٍ واحدٍ يراقب الاتصالات اللاسلكية من بلد أجنبي، أنظر أيضا، المحكمة الأوروبية، الطلب رقم 54934/00. 29 يونيو 2006، والتي وجدت المحكمة أن البلد المدعى عليه لم يتصرّف بطريقة تدخلت في السيادة الإقليمية البلدان الأجنبية كما هي محمية في القانون الدولي العام.

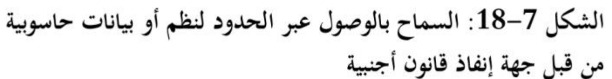
2 مجلس أوروبا، 2001. التقرير التفسيري لاتفاقية الجرائم السيبرانية.

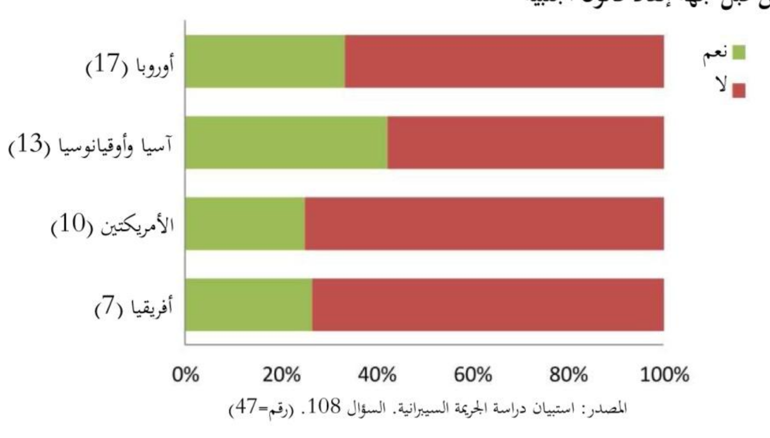
3 استبيان دراسة الجريمة السيبرانية. السؤال رقم 96.

4 استبيان دراسة الجريمة السيبرانية. السؤال رقم 108.

من البلدان المجيبة عن الاستبيان في أفريقيا، و 50 في المائة في أوروبا.[1] قد يعكس ارتفاع النسبة في أوروبا تأثير المادة 32(ب) من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية.

وفي الرد على الاستبيان، وضعت بلدان معنى واسعا على شرط الوصول "عبر الحدود" – مع بعض البلدان التي تشمل الوضع عندما تم تنفيذ الوصول المباشر إلى البيانات خارج الحدود بها، ولكن فقط بعد الحصول على موافقة وردت من السلطات الأجنبية.[2] كما أشار عدد من البلدان إلى قيودٍ معينة على هذه الممارسة، مثل الحاجة إلى الحصول على موافقة المالك وشروط الإخطار والحاجة لضمان أن البيانات مخزنةٌ بالفعل في الخارج. وقد استشهدت البلدان التي لم تستفد من الممارسة بشكل متكرر إلى عدم وجود الإطار القانوني كسبب رئيسي لعدم القيام بذلك. كما سلّطت بعض البلدان الضوء بشكل خاص على أنها كانت مقيّدة في جمع الأدلة من الخارج باستخدام المساعدة القانونية المتبادلة والإنابة القانونية.[3]


الشكل 7–18: السماح بالوصول عبر الحدود لنظم أو بيانات حاسوبية من قبل جهة إنفاذ قانون أجنبية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 108. (رقم=47)

وفيما يتعلّق بجواز وصول أجهزة إنفاذ القانون الأجنبية إلى أنظمة الحاسوب أو بياناته، ذكر نحو ثلثي بلدان العالم أن هذا شيء لا يجوز.[4] وقد ذكر بلدٌ واحد من أوقيانوسيا، على سبيل المثال، أن سلطات إنفاذ القانون الوطنية تستطيع "الوصول إلى أنظمة الحاسوب/وبيانات الحاسوب نيابة عن البلد الأجنبي من خلال عمليات المساعد القانونية المتبادلة الرسمية"، على الرغم من أن نطاق المساعدة "يقتصر على الحالات التي يتم فيها تنفيذ أمر التفتيش على المباني[الوطنية] [...]،" والسلطات الوطنية غير قادرة على "الوصول إلى الاتصالات المخزّنة بالنيابة عن البلد الأجنبي."[5] وتدرك بلدان أخرى أن الممارسة لم تكن تتفق مع مبدأ السيادة الدولية. عندما تسمح البلدان بالوصول عبر الحدود إلى أنظمة الحاسوب أو البيانات داخل أراضيها، تم ذكر ذلك في كثير من الأحيان ليكون على النحو المنصوص عليه في اتفاقية مجلس أوروبا بشأن الجريمة السيبرانة. وأشارت إحدى البلدان إلى أن الممارسة كان مسموح بها على أساس التبادل. وفي حالات أخرى، كما هو الحال بالنسبة لبلد واحد في أمريكا الجنوبية،

---

[1] المرجع نفسه

[2] المرجع نفسه

[3] المرجع نفسه

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 108.

[5] المرجع نفسه

فإن الممارسة مسموحٌ بها "في الحالات الملحّة التي تنطوي على جريمة خطيرة تهدد سلامة أو حياة الشخص.[1] وقد نوّهت بلدان أخرى إلى أن الوصول عبر الحدود يكون جائزا "إذا هددت المسألة الأمن القومي." فقد ذكرت إحدى بلدان شمال أوروبا أنه سيسمح بالوصول "في حالة استحالة معرفة [البلد] الذي تكون فيه البيانات في الواقع."[2]

ومن الناحية العملية، فإنه يبدو أن الدول المجيبة عن الاستبيان تعتمد عند الحصول على المعلومات عبر الحدود على القنوات الرسمية – استوجاب الطلبات للمساعدة القانونية المتبادلة.[3] وعموما، فإن أقل من 10 في المائة من البلدان قد نوهت إلى الاتصال "في الغالب" بمقدمي الخدمات خارح الإقليم مباشرة للحصول على أدلةٍ مثل بيانات المشترك وحركة السير والمحتوى.[4] أوضحت إحدى البلدان الواقعة في غرب آسيا أن الشروع في اتصال مع مقدّم الخدمة خارج الحدود يتم تنفيذه بطريقة غير رسمية، وإذا رفض مقدّم الخدمة التعاون فإن سلطات إنفاذ القانون تعود إلى القنوات الرسمية من أجل الحصول على الأذون اللازمة والبيانات المطلوبة.[5]

وضع مفاهيم الوصول المباشر إلى البيانات خارج الإقليم

من أجل وضع مفهوم الاعتبارات المتضمنة في الوصول إلى البيانات خارج الإقليم دون طلب مساعدة قانونية متبادلة رسمي، أو تعاون آخر غير رسمي بين شرطة وشرطة، يوضح الشكل التالي أربعة سيناريوهات ممكنة في سياق الحوسبة السحابية.

يشمل المثال مقدم الخدمة السحابية مع المقر الرئيسي ومراكز البيانات في البلد (ب)، ولكن مع مراكز بيانات إضافية في البلد (ج)، ومقرات إضافية في البلد (أ). تصل سلطات إنفاذ القانون في البلد (أ) أو تستلم بيانات سحابية يعتقد أنه تم تخزينها في البلد (ب) عن طريق:

(1) فرد يقع في البلد (أ) مع سيطرة على بيانات السحابة. يمكن الحصول على الوصول إما بسبب (1) موافقة الفرد، أو (2) استفادة السلطات من اتصال مباشر من جهاز الفرد.

(2) فرد يقع في البلد (ب) مع سيطرة على بيانات السحابة. يمكن الحصول على الوصول بسبب موافقة الفرد.

1 المرجع نفسه

2 المرجع نفسه.

3 استبيان دراسة الجريمة السيبرانية. السؤال رقم 105.

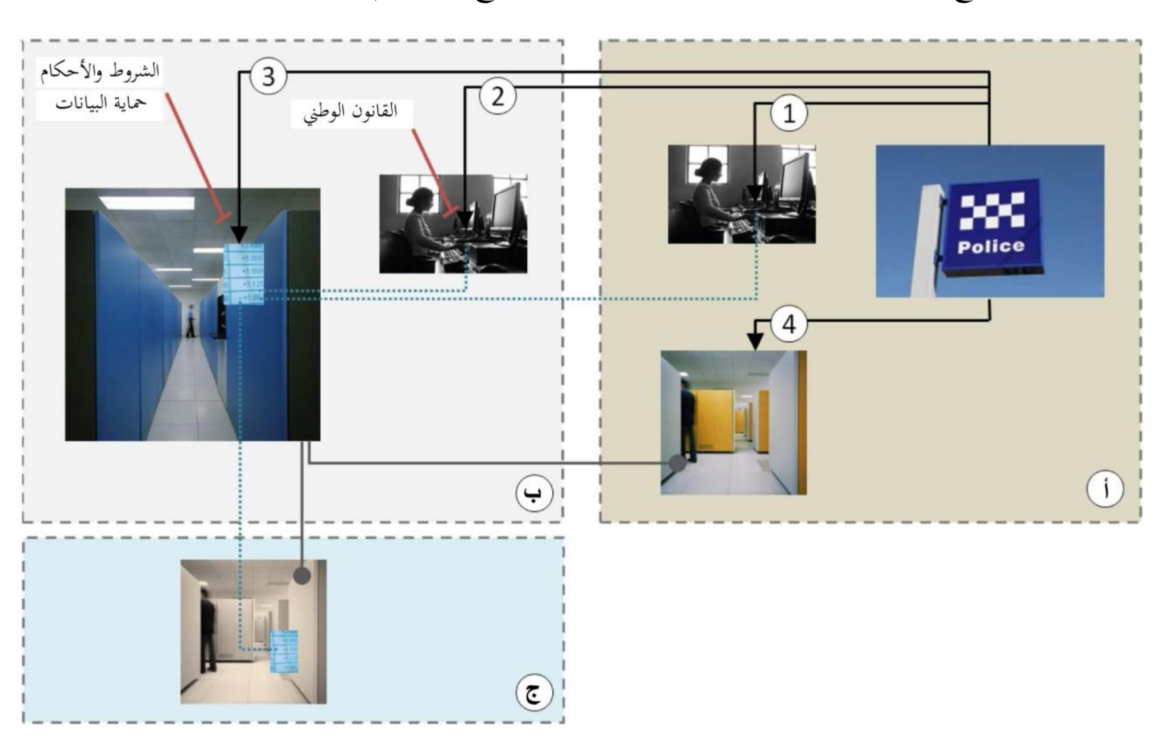
4 المرجع نفسه.

5 المرجع نفسه.

(3) مقدّم الخدمة السحابية في البلد (ب). يمكن الحصول على الوصول إما بسبب (1) موافقة مقدم الخدمة السحابية، أو (2) أوراق إعتماد وصول إلى البيانات تم الحصول عليها من قبل سلطات إنفاذ القانون.

(4) مقرّات مقدّم الخدمة السحابية في البلد (أ). يمكن الحصول على الوصول من خلال ترتيبات محلية غير رسمية بين سلطات إنفاذ القانون ومقدم الخدمة السحابية.

في كافة الحالات، بينما تعتقد سلطات إنفاذ القانون أن البيانات في حيازة مقدم الخدمات السحابية في مراكز البيانات الخاصة به في البلد (ب)، ومن الممكن أيضا أن تكون البيانات، أو نسخ منها، موجودة فعليا في البلد (ج). كما أنه في أمثلة أخرى محتملة قد لا تمتلك سلطات إنفاذ القانون في البلد (أ) معلومات أولية على الإطلاق بشأن موقع البيانات – بما في ذلك إذا ماكانت فعليّة خارج نطاقها أم لا.[1]



توضح مجموعة الاحتمالات مدى تعقيد الوصول المباشر من قبل سلطات إنفاذ القانون إلى البيانات خارج الحدود الإقليمية. فضمن المثال، توجد أيضا المزيد من الفروق البسيطة بما في ذلك: (1) تأثير شروط عميل مقدّم الخدمة السحابية وأحكامه على طلبات إنفاذ القانون الأجنبي. (2) قانونية التفاعل بين سلطات إنفاذ

1 خلال الوصول "المباشر" لجهاز المشتبه فيه، على سبيل المثال، قد لا يكون واضحا ما إذاكان يتم تخزين البيانات (أو "تخبئتها") محليّا على الجهاز، الوصول عبر اتصال شبكة اتصال إلى خادم خارج الإقليم.

القانون الأجنبي في البلد (ب) وبين الأفراد والأشخاص الاعتباريين داخل الإقليم، بالإضافة إلى (3) قانونية الطريقة التي يتم بها الحصول على أي اعتمادات الوصول من خلال إنفاذ القانون في البلد (أ).

بالنظر في مجموع من السيناريوهات المماثلة في تقرير صدر مؤخرا عن مجلس أوروبا وُجد عددٌ من الاختلافات في أساليب تعامل البلد. تم تضمين هذه الاختلافات في النهج مع الإشارة إلى: ما إذا كان من الواضح للمحققين أن البيانات تم تخزينها في سلطات قضائية مختلفة؛ ما إذا كان قد تم السماح للمحققين في الحصول على حق الوصول عن بعد عن طريق برامج مثل كيلوجرز وسنيفرز؛ ما إذا كان الشخص الذي يقدم الوصول لديه السلطة القانونية للإفصاح عن البيانات بموجب القوانين في المكان الذي يتم فيه تخزين البيانات؛ وعما إذا كان يحدث فرق إذا كان الشخص الذي يقدّم الوصول يقع فعلا في الدولة المطالبة أو خارج إقليمها.[1]

الاعتبارات الرئيسية

سلّط المثال الافتراضي الذي تم التنويه إليه أعلاه جنبا إلى جنبٍ مع إجابات البلدان عن استبيان الدراسة الضوء على عدد من الاعتبارات الرئيسية.

أولا: من الواضح أن سلطات إنفاذ القانون قد تصل بشكل مباشر، في الممارسة، إلى البيانات خارج الحدود دون الحصول على موافقة من أي فرد أو مقدم للخدمة. وهذا قد يحدث على سبيل المثال، عندما يستفيد المحققون من اتصال مباشر موجود من جهاز المشتبه فيه، أو عندما يستخدم المحققون أوراق اعتماد الوصول إلى البيانات التي تم الحصول عليها بشكل قانوني للوصول إلى البيانات السحابية.

ثانيا: لن يكون بوسع سلطات إنفاذ القانون التي تنفذ مثل هذه الأعمال أن تعرف دائما ما إذا كان الوصول إلى البيانات في الحقيقة خارج أراضيها، أو إذا كانت كذلك، في أي بلد أو بلدان تقع. يمكن أن يحدث هذا، على سبيل المثال، عندما يقوم مقدمو خدمة الحوسبة السحابية بتخزين البيانات في مسخ متعددة في مراكز البيانات في بلدان مختلفة، ويقوموا بالاستفادة من الإدارة الديناميكية للبيانات بين مراكز البيانات هذه.

لكلا هاتين النقطتين صلة بالنهج الدولية والإقليمية القائمة مثل أحكام المادة 32(ب) من اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، والمادة 40(2) من اتفاقية جامعة الدول العربية – وكلاهما يتطلّب موافقة شخص له سلطة قانونية للكشف عن البيانات، ومقصورٌ على الوصول التصوري إلى البيانات الواقعة في طرفٍ آخر. لا تغطي مثل هذه الأحكام الوضع عندما لا يتم الحصول على الموافقة وتكون البيانات تقع بشكل فعلي في بلدٍ ليس طرفا في المعاهدة ذات الصلة.

[1] مجلس أوروبا، لجنة إتفاقية الجريمة السيبرانية (T-CY)، المجموعة الفرعية المخصصة في الولاية القضائية والوصول إلى البيانات عبر الحدود 2012. الوصول عبر الحدود والولاية القضائية: ما هي الخيارات؟ T-CY (2013) 3-6 ديسمبر، الصفحة 29-31.

وبشكل خاص، فيما يتعلق بمسألة الموافقة ومقدمي الحوسبة السحابية – نوهت العديد من البلدان المجيبة عن الاستبيان أن مقدمي الخدمات العاملين في نطاق الولاية القضائية الخاصة بهم ملزمون فقط بالكشف عن البيانات بناء على إيصال أمر من المحكمة أو استدعاء أو أمر قضائي.[1] تنطبق هذه الالتزامات – إن لم يكن أكثر من ذلك – لطلبات إنفاذ القانون الأجنبية. كما أشار عدد من مقدمي الخدمة الذين أجابوا عن الدراسة إلى أنهم لا ينظرون إلى الطلبات غير الرسمية من سلطات إنفاذ القانون الأجنبية ليحدثوا أي التزام بخصوص الكشف عن البيانات.[2] وعموما، نوّهت الشركات المجيبة عن الدراسة إلى أنها فضّلت تلقّي طلبات رسميةٍ من خلال الأنظمة القائمة على معاهدات المساعدة القانونية المتبادلة. كما أوضحت دراسةٌ للمبادئ التوجيهية من مقدمي خدمة الإنترنت أيضا هذا الأسلوب. وتنص المبادئ التوجيهية لإنفاذ القانون من تويتر، على سبيل المثال، على أن "... القانون يخوّل تويتر للرد على طلبات الحصول على معلومات المستخدم من جهات إنفاذ القانون الأجنبية التي تصدر عن طريق .... المحكمة إما عن طريق معاهدة للمساعدة القانونية المتبادلة أو عن طريق الإنابة القضائية."[3] على هذا النحو، قد تجد سلطات إنفاذ القانون الأجنبية صعوبة في الحصول على البيانات من مقدّم الخدمة خارج الحدود بموافقة مباشرة.

تصل الصورة إلى واحدٍ من التوازنات المعقدة. فمن ناحية، تشير بعض حجج (نقاشات) السيادة والخصوصية الفردية إلى أن الوصول إلى بيانات الحاسوب خارج الإقليم لا يكون مناسبا إلا من خلال إجراءات المساعدة القانونية المتبادلة – والتي يرتب عليها النظر رسميا في مثل هذه القضايا على أساس كل قضية على حدة.[4] ومن ناحية أخرى، فإن حقائق إنفاذ القانون تشير إلى أن الوصول، من خلال عدد من الوسائل، إلى البيانات خارج الإقليم يحدث، في الممارسة، في سياق التحقيقات – إما من خلال المحققين أو بدون علمهم. تشمل القوى الدافعة لذلك طول الفترة الزمنية المطلوبة لإجراءات التعاون الرسمية؛ الحالات التي يتم فيها مواجهة الأجهزة ذات الاتصال المباشر؛ وعندما تصبح أوراق اعتماد الوصول معروفة أثناء التحقيق.

تمثّل النهج الدولية والإقليمية الحالية عددا من القيود من خلال التركيز على "الموافقة" والمعرفة المفترضة "لموقع" البيانات. في الواقع، من النادر معرفة الموقع "الحقيقي" للبيانات في بداية التحقيق، أو في النقطة التي قد يكون فيها إلى الوصول إلى البيانات مطلوبا. حتى عندما تستخدم طلبات المساعدة القانونية المتبادلة الرسمية، قد تكون هذه الطلبات موجهة إلى السلطة القضائية لمركز مقدم الخدمة السحابية بدلا من السلطة القضائية للمركز الفعلي للبيانات.[5]

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 21.

[2] استبيان دراسة الجريمة السيبرانية (القطاع الخاص). السؤال رقم 21.

[3] أنظر http://support.twitter.com/articles/41949-guidelines-for-law-enforcement#

4 قدمت هذه التوصية، على سبيل المثال، من خلال مبادرة الشبكة العالمية 2012. الحريات الرقمية في القانون الدولي: خطوات عملية في حقوق الإنسان على الإنترنت.

5 قدرة الاتفاقيات بين مشغلي مراكز البيانات التي تملكها الشركات العالمية والبلدان المضيفة على معالجة هذه النقطة.

من منظور منع الجريمة والعدالة الجنائية، تتواجد عدد من الظروف التي يكون فيها الوصول الملحّ إلى البيانات السحابية مطلوبا – بما في ذلك عند وجود تهديد وشيك بالضرر. يتطلّب تحقيق توافق في الآراء بشأن الطريقة الأكثر فعالية التي قد يتحقق بها إحراز ذلك مع ضمان احترام حقوق الإنسان الفردية ما يلي:[1] (1) إعادة صياغة مفهوم إلى أيّ مدى يمكن استخدام "موقع البيانات" كقاعدة توجيهية. (2) تطوير المعايير المشتركة والضّمانات المتعلّقة بالملابسات، إن وجدت، التي بموجبها قد يتم الوصول المباشر إلى البيانات خارج الحدود من قبل المكلّفين بإنفاذ القانون.

1 أنظر الفصل الخامس (إنفاذ القانون والتحقيقات) القسم 5-3 الخصوصية وإجراءات التحقيق.

الفصل الثامن: منع الجريمة السيبرانية

يلقي هذا الفصل نظرة شاملة على منع الجريمة السيبرانية من منظور الحكومات والقطاع الخاص فضلا عن الأوساط الأكاديمية، حيث يقيم العديد من الروابط بين أصحاب المصالح ويؤكد على مجموعة من التفاعلات بينها والتي من شأنها أن تؤدي إلى تدابير فعّالة لمنع الجريمة السيبرانية.

1-8 منع الجريمة السيبرانية والاستراتيجيات الوطنية

الاستنتاجات الرئيسية:

- أفاد 40 في المائة من البلدان المجيبة بوجود قانون وطني أو سياسة وطنية لمنع الجريمة السيبرانية. وما زالت المبادرات قيد الإعداد في 20 في المائة من البلدان
- تشمل الممارسة السليمة إصدار التشريعات، والقيادة الفعّالة، وتطوير العدالة الجنائية وقدرة إنفاذ القانون، والتعليم والوعي، فضلا عن تطوير قاعدة معرفية قوية، وكذلك التعاون عبر الحكومة والقطاع، الخاص وعلى المستوى الدولي
- أفاد حوالي 70 في المائة من جميع البلدان أن الاستراتيجيات الوطنية تشمل العناصر الخاصة برفع مستوى الوعي والتعاون الدولي والقدرة على إنفاذ القانون
- أفاد أكثر من 50 في المائة من البلدان بأنها أقامت شراكات بين القطاع العام والخاص لمنع الجريمة السيبرانية ومكافحتها

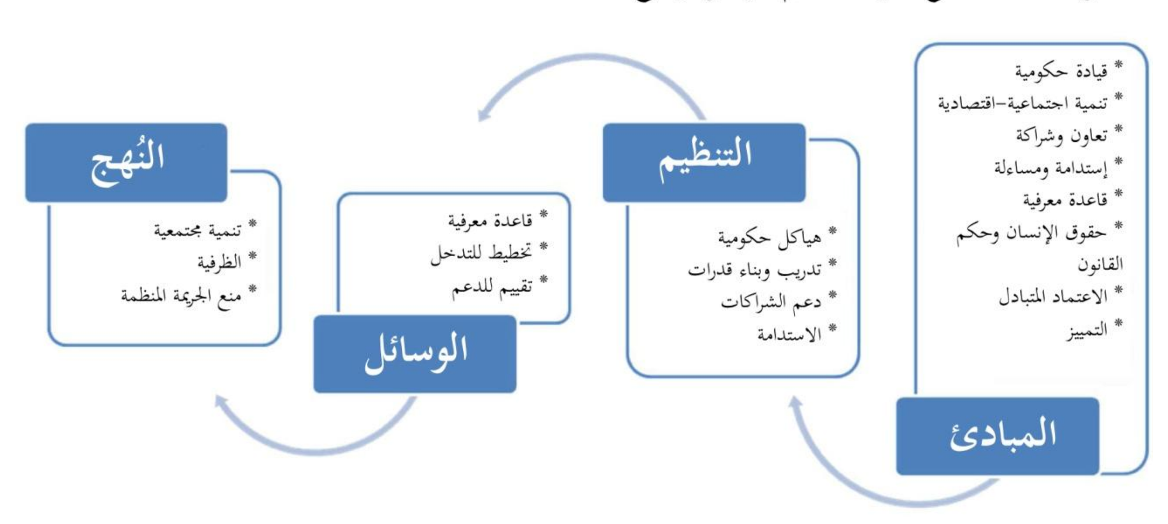
مقدمة لمنع الجريمة

يشير مصطلح "منع الجريمة" إلى الاستراتيجيات والتدابير التي ترمي إلى تقليل خطر الجريمة وتأثيراتها الضارة والمحتملة على الأفراد والمجتمع من خلال التدخلات التي توثر على الأسباب المتعددة للجريمة.[1] وتسلط مبادئ الأمم المتحدة التوجيهية لمنع الجريمة الضوء على أن قيادة الحكومة تلعب دورا هاما في منع الجريمة مع التعاون والشراكات عبر الوزارات وبين السلطات والمنظمات المجتمعية والمنظمات غير الحكومية وقطاع الأعمال

[1] المبادئ التوجيهية لمنع الجريمة، مرفق قرار المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة 2002/13 بشأن تدابير تعزيز منع الجريمة منعا فعالا 24 يوليو 2002، الفقرة 3.

التجارية والمواطنين العاديين.[1] وتبدأ الممارسة السليمة لمنع الجريمة *بالمبادئ* الأساسية (مثل القيادة والتعاون وسيادة القانون)، مما يسمح باقتراح أشكال *للتنظيم* (مثل خطط منع الجريمة)، وتؤدي إلى تنفيذ *الأساليب* (مثل تطوير قاعدة معارف سليمة) وكذلك *النُّهج* (التي تشمل خفض الفرص الجنائية وتحصين الهدف).

الشكل 8–1: مبادئ منع الجريمة، التنظيم، الوسائل، والنهج



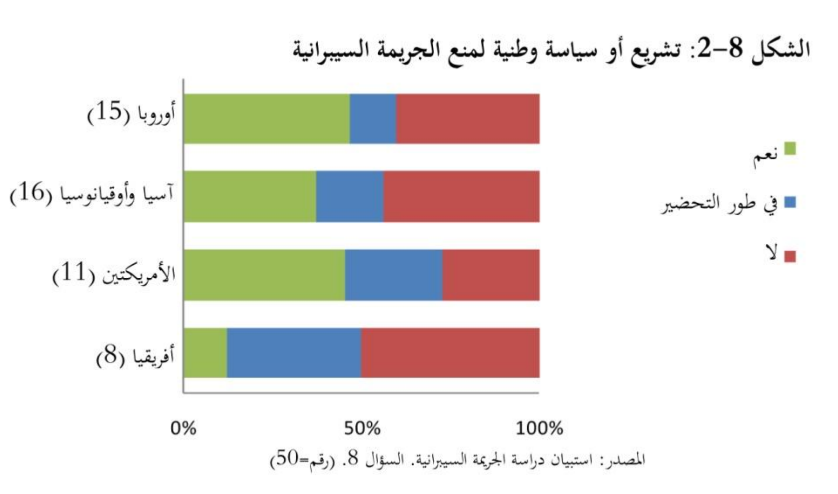
تمثل الجريمة السيبرانية تحديات خاصة في طريق منع الجريمة. ويشمل هذا تزايد القدرة الاقتنائية لأجهزة الإنترنت وتوفرها في كل مكان، الأمر الذي يؤدي إلى وجود عدد كبير من الضحايا المحتملين، وكذلك رغبة الأشخاص في القيام بسلوك "خطر" على الإنترنت مقارنة بما كان عليه الأمر في السابق ؛ وتقنيات إخفاء الهوية والتشويش من جانب مرتكبي الجرائم، والطبيعة العابرة للحدود للكثير من الأفعال المنطوية على جريمة سيبرانية، وسرعة وتيرة الابتكار الجنائي. ويسهم كل تحدي من هذه التحديات بتأثيراته على التنظيم والأساليب والنهج المتبعة لمنع الجريمة السيبرانية؛ إذ يتعين على الهياكل التنظيمية، على سبيل المثال، أن تعكس الحاجة إلى تعاون دولي وإقليمي في منع الجريمة السيبرانية. ويتعين على *الأساليب* أن تضمن صورة محدثة باستمرار للمخاطر السيبرانية، كما يتعين على *النهج* أن تتضمن مجموعة من أصحاب المصالح، وعلى وجه التحديد منظمات القطاع الخاص التي تملك وتشغل البنية التحتية للإنترنت وخدماتها.

النهج الوطنية لمنع الجريمة السيبرانية

تتجسد إحدى الأوجه المتكاملة للجانب *التنظيمي* لمنع الجريمة في وضع *خطة* لمنع الجريمة ذات أولويات وأهداف واضحة.[1] وتنص المبادئ التوجيهية لمنع الجريمة على أن تقوم الحكومات بتضمين المنع كجزء دائم في

[1] المرجع نفسه. المواد 7 و 9.

هياكلها وبرامجها الرامية إلى السيطرة على الجريمة، وكذلك ضمان وجود مسؤوليات محددة *وأهداف* واضحة داخل الحكومة لتنظيم منع الجريمة.[2]



الشكل 8–2: تشريع أو سياسة وطنية لمنع الجريمة السيبرانية

المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 8. (رقم=50)

وقد أشارت حوالي 40 في المائة من البلدان المجيبة، أثناء جمع المعلومات الخاصة بالدراسة، إلى وجود تشريعات وطنية أو سياسة خاصة بمنع الجريمة السيبرانية.[3] كما أشارت 20 في المائة أخرى من البلدان بأن القانون أو السياسة قيد التطوير. وأفادت بلدان في أوروبا والأمريكتين غالبا بوجود قانون أو سياسة تخص منع الجريمة. وأفاد عدد قليل من البلدان بوجود قانون أو سياسة لمنع الجريمة، على الرغم من أن حوالي 40 في المائة من البلدان المجيبة من أفريقيا أفادت بأن تلك الوسيلة قيد التطوير. وعلى الصعيد العالمي أكّد أكثر من نصف مجموع البلدان المجيبة على أن عدم وجود تشريع أو سياسة وطنية لمنع الجريمة السيبرانية يشير إلى وجود إمكانيات كبيرة لتعزيز الإجراءات في هذا المجال.

وبخصوص البلدان التي تتوفر على قوانين أو سياسات خاصة بمنع الجريمة السيبرانية، أفادت هذه البلدان بأن الهدف من وراء وضع قوانين وسياسات منع الجريمة السيبرانية هو "*تنظيم البيئة القانونية وتنسيقها، ووضع نظم مؤسسية فعالة ومنسقة، وإسناد مسؤوليات الأوجه المختلفة للجريمة السيبرانية، وإعداد برامج توعية للمستخدمين والكوادر الفنية وصناع القرار*".[4] وأكدت بلدان أخرى أيضا على أن قوانين المنع تحدد الأدوار المختلفة ومسؤولية المؤسسات العامة ومزودي الخدمة والمنظمات غير الحكومية في برامج منع الجريمة السيبرانية.

ونوه عدد من البلدان – في كل من دول العالم المتقدم والنامي – إلى ما تقوم به في مجال منع الجريمة السيبرانية أو أنشطة التوعية التي يتم إجراؤها بما في ذلك من خلال وكالات إنفاذ القانون والمؤسسات الحكومية الأخرى والأوساط الأكاديمية ومنظمات القطاع الخاص. وأفادت إحدى البلدان في أمريكا الجنوبية بالعمل مع

---

[1] المبادئ التوجيهية لمنع الجريمة، مرفق قرار المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة 2002/13 بشأن تدابير تعزيز منع الجريمة منعا فعالا 24 يوليو 2002، الفقرة 17.

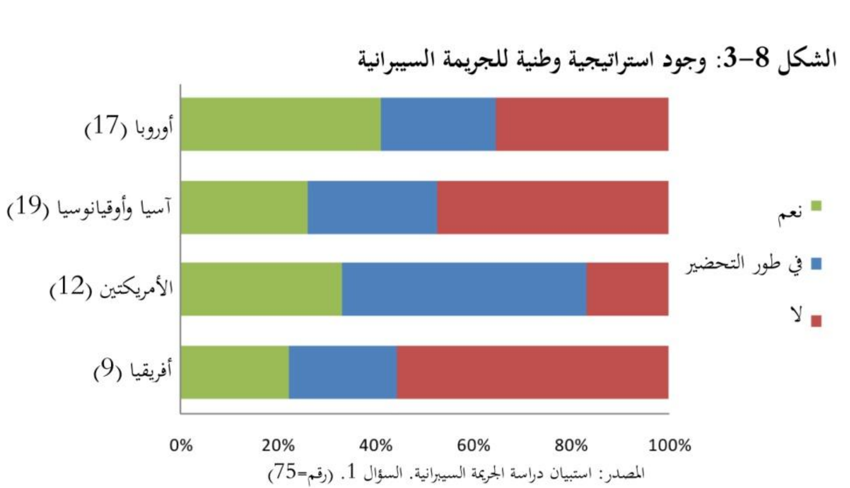
[2] المرجع نفسه.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 8.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 8.

مقدمي خدمة الإنترنت ومقاهي الإنترنت على الامتثال للقوانين التنظيمية وكذلك أنشطة الحد من المخاطر في مجتمعات محددة من خلال تشكيل لجان منع الجريمة التي تهدف إلى تعزيز منع الجريمة الرقمية.[1] وأبرزت بلدان أخرى العمل مع اتحادات البنوك على تعزيز أمن الإنترنت، وتطوير تدريب الأمن السيبراني بالشراكة مع المنظمات غير الحكومية في المدارس وتفاعل وكالات إنفاذ القانون في المؤتمرات والمنتديات الأخرى الخاصة بالجريمة السيبرانية.[2] وأشارت البلدان أيضا إلى أهمية تحديد نقطة اتصال للمواطن يمكنه الوصول إليها بسهولة وكذلك تقارير الشركات عن الجريمة السيبرانية والحصول على نصائح منعها. وستجري مناقشة أنشطة رفع مستوى التوعية بالتفصيل لاحقا في هذا الفصل.

استراتيجيات الجريمة السيبرانية



الشكل 8-3: وجود استراتيجية وطنية للجريمة السيبرانية

وضع العديد من البلدان إجابات متعلقة *بمنع* الجريمة السيبرانية ضمن السياق العام للاحتياج إلى *استراتيجية* قومية للجريمة السيبرانية.[3] في المقابل، أكدت كثير من البلدان أيضا على الروابط القوية بين *الجريمة السيبرانية* واستراتيجيات *الأمن السيبراني*. وعند السؤال عن وجود استراتيجية وطنية (أو نظيرة لها) لـ "الجريمة السيبرانية"، أشارت البلدان إلى جميع الاستراتيجيات "السيبرانية" واستراتيجيات "الأمن السيبراني"، واستراتيجيات "أمن المعلومات"، واستراتيجيات "الفضاء السيبراني"، واستراتيجيات "الجريمة السيبرانية".[4] وتؤكد هذه المجموعة من الإجابات على الترابط المتزايد بين أمن المواطن والتعرض للجريمة السيبرانية، وأمن البنية التحتية الحاسوبية الوطنية، وكذلك أمن الشركات عبر الوطنية. وعلى الرغم من أن وجود تداخل كبير بين نهج الجريمة السيبرانية والأمن السيبراني، إلا أن كلا المجالين يحظيان بوجود بعض الاختلافات. ويمكن تلخيص هذا في المربع الموجود في هذه الصفحة.

---

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 9.

[2] المرجع نفسه.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 1 ورقم 8.

[4] استبيان دراسة الجريمة السيبرانية. السؤال رقم 1.

وبقدر ما أفادت البلدان المجيبة حول مجموعة من الاستراتيجيات ذات الصلة بالجريمة السيبرانية، فإن التحليل في هذا الفصل لا يقتصر على تعريف "دقيق" لاستراتيجية الجريمة السيبرانية، بل يسعى لأن يعكس المعلومات المقدمة من خلال استبيان الدراسة، وأن يشمل جميع أنواع الاستراتيجيات المبلغ عنها.

وعموما، أشار حوالي 30 في المائة من البلدان المجيبة إلى وجود استراتيجية وطنية للجريمة السيبرانية (بالمعنى الأوسع). ووفقا للمنطقة أفاد ما بين 20 إلى 50 في المائة من البلدان بوجود استراتيجية قيد الإعداد. وأفادت بلدان في أفريقيا وآسيا وأوقيانوسيا بأقل مستويات من استراتيجيات الجريمة السيبرانية – مع إشارة 50 في المائة أو أكثر من البلدان إلى عدم وجود تلك الوسيلة. وتعتبر استراتيجيات الجريمة السيبرانية مهمة للتأكد من أن إجابات إنفاذ القانون الوطني والعدالة الجنائية تأخذ في الحسبان تماما التحديات الخاصة بالجريمة السيبرانية وكذلك عناصر الأدلة الإلكترونية لجميع الجرائم. ويمثل تطوير استراتيجية الجريمة السيبرانية خطوة أولية هامة في تحديد الأولويات الاستراتيجية والتشغيلية قبل المشاركة في عمليات مثل الإصلاح التشريعي. وكما يتضح من خلال مجموعة من أجوبة البلدان، فإنه يمكن إعداد الاستراتيجيات الخاصة بالجريمة السيبرانية باعتبارها وثائق قائمة بذاتها أو إدماجها باعتبارها من عناصر الاستراتيجيات الخاصة بالأمن السيبرانية.

استراتيجيات الجريمة السيبرانية والأمن السيبراني

المصالح الوطنية والأمن والثقة والمرونة وموثوقية تكنولوجيا المعلومات والاتصالات		سيادة القانون، وحقوق الإنسان، ومنع الجريمة، والعدالة الجنائية	
استراتيجيات الأمن السيبراني		**استراتيجيات الجريمة السيبرانية**	
الحوادث الأمنية غير المتعمدة لتكنولوجيا المعلومات والاتصالات	الهجمات المتعمدة ضد سرية نظم الحاسوب والبيانات وسلامتها وتوفرها	الجرائم المتعلقة بالحاسوب والمحتوى	أي جريمة تنطوي على أدلة إلكترونية

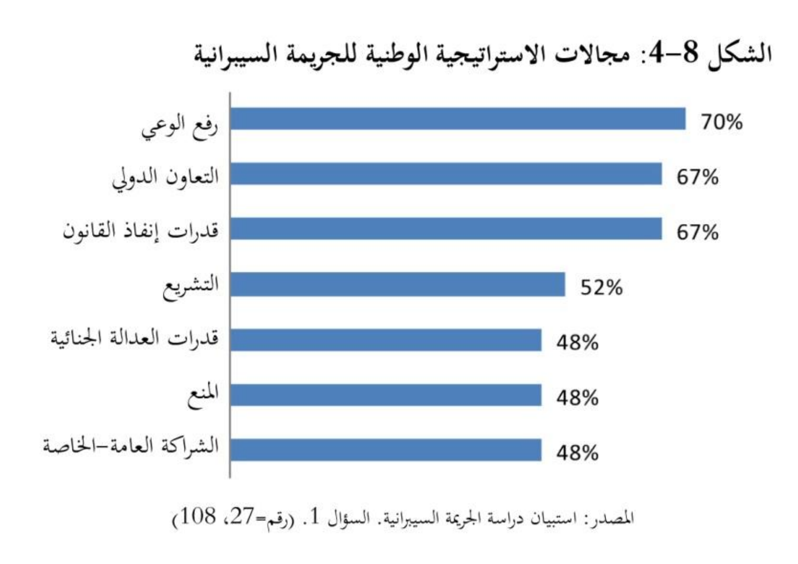
Adapted from Seger, A. 2001. *Cybercrime strategies. Octopus conference*

وخلال جمع معلومات الدراسة، سُئلت البلدان عن المجالات التي تغطيها استراتيجيات الجريمة السيبرانية. وتشمل المجالات المبلغ عنها جميع تلك المجالات التي تم تناولها في هذه الدراسة، بما في ذلك منع الجريمة السيبرانية وزيادة مستوى الوعي، والقدرة على إنفاذ القانون والعدالة الاجتماعية، والشراكات بين القطاع العام والخاص، والتشريعات والتعاون الدولي. ويمثل منع الجريمة عنصرا أساسيا لما يقرب من 30 استراتيجية وطنية يتم تقديم المعلومات المتعلقة بها. وعموما، تم إدراج "منع" الجريمة السيبرانية فيما يقرب من نصف الاستراتيجيات الوطنية المبلغ عنها ككل. بالإضافة إلى ذلك، فإن المجال الأكثر ذِكرا والذي شملته تلك الاستراتجيات هو نشاط المنع

الخاص بـ "زيادة الوعي" – وتشمل 70 في المائة من الاستراتيجيات المبلغ عنها هذا الموضوع.[1] ويستعرض القسم التالي في هذا الفصل هذا المجال بالتفصيل.

التعاون الدولي هو المجال التالي الأكثر ذِكرا وشيوعا ضمن الاستراتيجيات الوطنية المبلغ عنها للجريمة السيبرانية. وأكد عدد من البلدان على الأهمية الاستراتيجية لهذا المجال، بما في ذلك منظور منع الجريمة السيبرانية. وأشارت إحدى البلدان إلى أنه: *"يُنظر للتعاون الدولي باعتباره الركن الأساسي للتحديات الكبيرة التي يفرضها الإجرام السيبراني الذي يتميز بكونه عبر وطني وعالي السرعة فضلا عن كونه معقدا ومنتشرا في جميع الدول الأعضاء التي يتعين عليها تحقيق توازن بين الحاجة لتحقيق سريع وفعال وتدابير إنفاذ القانون مقابل حماية السيادة الوطنية فضلا عن احترام المعاملات والحاجة لضمان حماية حقوق الإنسان للأشخاص الخاضعين لولايتها القضائية"*.[2] وتتم مناقشة التعاون الدولي في الأمور الجنائية المشتملة على جريمة سيبرانية في الفصل السابع (التعاون الدولي) من هذه الدراسة.

الشكل 8–4: مجالات الاستراتيجية الوطنية للجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 1. (رقم=27، 108)

ونفس النسبة (ما يقرب من 70 في المائة) من البلدان شملت "قدرة إنفاذ القانون" ضمن المجال الرئيسي لاستراتيجيتها الوطنية بشأن الجريمة السيبرانية. وتصف إحدى البلدان التحديات المبلغ عنها بخصوص القدرة على إنفاذ القانون بأنها تتمثل في *"الأدوات، والقدرة، وحقوق الإنسان"*.[3] ويدرس الفصل الخامس (إنفاذ القانون والتحقيقات) من هذه الدراسة هذا المجال بشكل أكثر تفصيلا. وتشمل المجالات الأخرى، الواردة في الاستراتيجيات الوطنية الخاصة بالجريمة السيبرانية، تشريعات الجريمة السيبرانية، والقدرة على تحقيق العدالة الجنائية. وظهر اهتمام مشترك حول ترسيخ إمكانيات وتعليم المدعين العامين، والقضاة وموظفي القضاء. وحدّدت بعض الدول أهدافا وخططا محددة مثل وضع *"نائب عام واحد على الأقل مسؤول حصريا عن قضايا الجريمة السيبرانية*

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 1.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 4.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 5.

في جميع المحاكم الابتدائية بحلول 2015" [1] أو أن *"تشكل مجموعة من الخبراء القضائيين من القطاع العام والخاص لتبادل الخبرات والمعرفة."* [2] ويدرس الفصل السادس (الأدلة الإلكترونية والعدالة الجنائية) هذا المجال.

ويتجلى الموضوع الآخر والمحدد عادة في أولويات منع الجريمة السيبرانية في أهمية حماية البنى التحتية الوطنية الهامة. تم التنبيه على هذا حتى يشمل *"تطوير معايير المعلومات والأمن السيبراني والوعي، وكذلك آليات تحديد التهديدات السيبرانية والتخفيف من حدتها."* [3] ويوصف التعاون في هذا الصدد، بين الحكومة الفيدرالية والمحلية والقطاعات الأخرى، على وجه الخصوص، باعتباره ضروريا *"لتسهيل تبادل المعلومات المتعلقة بأفضل الممارسات، ومعلومات التحقيق، وتنسيق التعامل مع الحوادث، وإدارة الحوادث والإجراءات والعمليات"* . [4]

قيادة الجريمة السيبرانية

إعترفت البلدان المجيبة أن مجموعة من المؤسسات والهيئات الحكومية مطلوب منها دعم منع الجريمة وتدابير العدالة الجنائية في مجال الجريمة السيبرانية. إلا أن العديد من البلدان أشارت إلى أن منع الجريمة السيبرانية يتطلب قيادة مركزية وتعزيزا للموارد لتنسيق المبادرات الحكومية لمنع الجريمة السيبرانية.[5] وأشار 75 في المائة من البلدان المجيبة إلى أنها قامت بتحميل مؤسسة حكومية رائدة مسؤولية منع الجريمة السيبرانية ومكافحتها.[6] وكانت المؤسسة التي عادة ما يتم الإشارة إليها (في حوالي 30 في المائة من الدول المجيبة) هي الشرطة الوطنية أو سلطات إنفاذ القانون. وتشمل المؤسسات الأخرى التي عادة ما تُعرف ريادتها، مكاتب المدعي العام أو النائب العام ووزارات العدل. فضلا عن الإبلاغ عن التنسيق "متعدد الوكالات" في أكثر من 10 في المائة من البلدان.[7]

تم الإبلاغ في نسبة قليلة من البلدان (حوالي 10 في المائة أو دونها) عن دور التنسيق الريادي في مجال الجريمة السيبرانية الواقعة على عاتق وزارات الاتصالات، ووكالات الأمن السيبراني، أو أفرقة التصدي للطوارئ الحاسوبية، بدلا من مؤسسات منع الجريمة والعدالة الجنائية.[8] وتلعب أفرقة التصدي للطوارئ الحاسوبية دورا أساسيا في تحديد نقاط ضعف النظام الحاسوبي، وكذلك التصدي لحوادث الأمن الحاسوبي.[9] ونتيجة ذلك، يمكنها أن تحظى بنظرة ثاقبة في اتجاهات الجريمة السيبرانية الحالية. ويؤكد استخدام وزارات الاتصالات وأفرقة التصدي

[1] المرجع نفسه.

[2] المرجع نفسه.

[3] المرجع نفسه.

[4] المرجع نفسه.

[5] المرجع نفسه.

[6] استبيان دراسة الجريمة السيبرانية. السؤال رقم 2.

[7] المرجع نفسه.

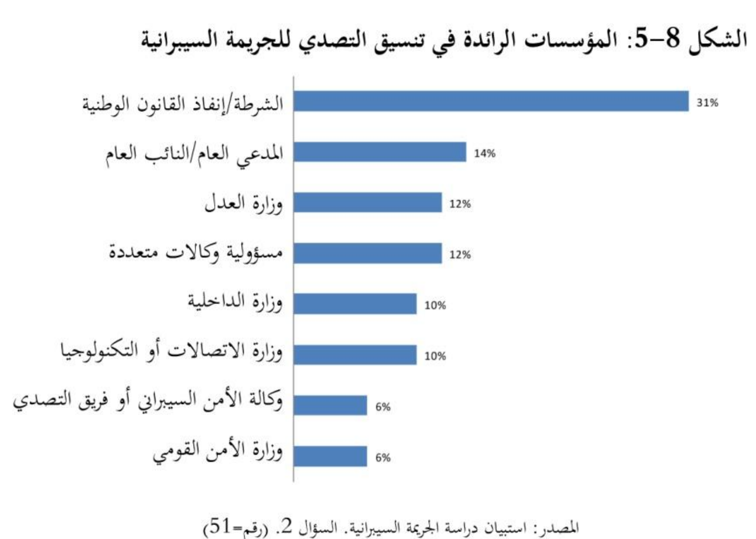
[8] المرجع نفسه.

[9] مكتب تقييس الاتصالات، 2012. قرار 58- تشجيع إنشاء فرق فريق الاستجابة لحوادث الحاسوب، خاصة للبلدان النامية.

للطوارئ الحاسوبية بوصفها رائدة في مجال الجريمة السيبرانية على الطبيعة متعددة الاختصاصات لعملية التصدي للجريمة السيبرانية.

ومع ذلك، فمن الجدير بالذكر بالنسبة للجزء الأكبر أن التنسيق الرائد يعكس في المقام الأول توصيف الجريمة السيبرانية باعتبارها تحديا أمام إنفاذ القانون والعدالة الجنائية بدلا من أن تمثل تحديا تكنولوجيا أو تحديا للاتصالات. وعلى الرغم من هذا، فإن الجريمة السيبرانية تنطوي على عناصر من كليهما، ويشير العمل الحالي على المستوى الأوروبي إلى أهمية التعاون بين أفرقة التصدي للطوارئ الحاسوبية وإنفاذ القانون في مجالات الاستجابة للحوادث وتبادل المعلومات.[1] وأكدت بعض البلدان التي أجابت على استبيان الدراسة على هذا المجال أيضا. كما أكدت البلدان مرارا وتكرارا على سبيل المثال على أهمية النهج التعاوني بسبب تعقيد مخاطر الجريمة السيبرانية، بما في ذلك البنية التحتية الاقتصادية الهامة. وفي هذا الصدد، تشمل التحديات المحددة في التنسيق الفعّال لأنشطة منع الجريمة السيبرانية، عدم وجود إحصاءات رسمية وبيانات موثوقة حول مدى استفحال الجريمة السيبرانية، وعدم وجود تشريعات ذات صلة، فضلا عن *"عدم وجود تبادل للمعلومات، والتنسيق والتعاون بين أصحاب المصالح وتداخل أدوار الهيئات الحكومية لتكنولوجيا المعلومات"*.[2]

الشكل 8-5: المؤسسات الرائدة في تنسيق التصدي للجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 2. (رقم=51)

---

[1] الشبكة الأوروبية ووكالة أمن المعلومات، 2012. مكافحة الجريمة السيبرانية: التعاون بين فرق التصدي للطوارئ الحاسوبية ووكالات إنفاذ القانون في مكافحة الجريمة السيبرانية. أول مجموعة من الممارسات.

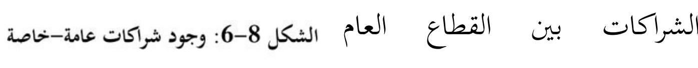
[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 5.

الشراكات بين القطاع العام والخاص

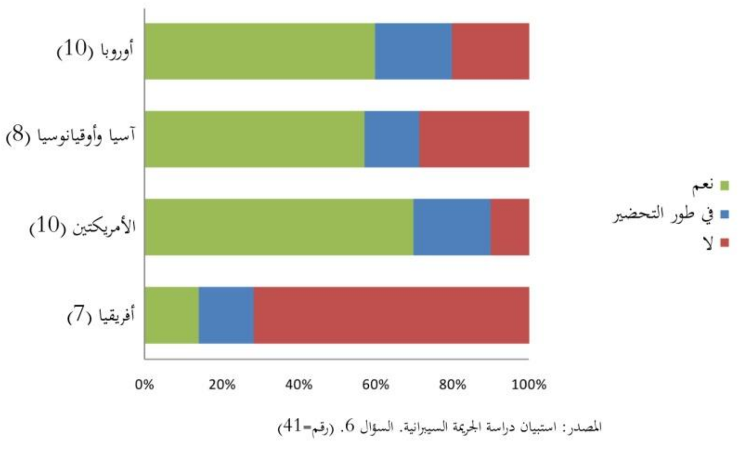
بالإضافة إلى الشراكة والتعاون داخل الحكومة، أكدت البلدان المجيبة في جميع أنحاء المناطق على أهمية الشراكات بين القطاع العام والخاص. وبشكل عام، أفادت أكثر من 50 في المائة من البلدان المجيبة بإقامة شراكات بين القطاع العام والخاص لمنع الجريمة السيبرانية ومكافحتها. وأفادت أقل من 20 في المائة من البلدان المجيبة أن الشراكات كانت قيد الإعداد. في حين أفادت حوالي 30 في المائة من البلدان المجيبة بعدم وجود شراكات بين القطاع العام والخاص.[1]

وتقع غالبية البلدان التي تفيد بعدم وجود شراكات في كل من أفريقيا وآسيا وأوقيانوسيا. كما أفادت أكثر من 60 في المائة من البلدان المجيبة من أفريقيا بعدم وجود شراكات بين القطاع العام والخاص. ونجد هذه الصورة معكوسة في أوروبا والأمريكتين، حيث أفادت 60 في المائة أو أكثر من البلدان المجيبة بوجود شراكات ذات صلة.

وأشارت البلدان إلى عدد من العوامل المحفزّة لإقامة الشراكات،



الشكل 8-6: وجود شراكات عامة-خاصة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 6. (رقم=41)

نماذج للشراكات بين القطاعين العام والخاص المتعلقة بالجريمة السيبرانية

تعتبر الأطر القانونية والثقة والحوافز وعوامل أخرى هامة باعتبارها عوامل تساعد على إقامة شراكات قوية بين القطاعين العام والخاص في مجال الأمن السيبراني. ويكون الاهتمام بتحليل النموذج الأفضل لتحقيق شراكة ناجحة في إطار يمكنه تقليص التحديات وتوفير أعظم استفادة. وقد ظهرت خمس نماذج أساسية:

- تبادل المعلومات غير الربحية على المستوى العالمي
- تبادل المعلومات الموزعة على صعيد المجتمع المحلي
- تبادل المعلومات المركزية على صعيد المجتمع المحلي
- الحكومة المغلقة
- التعاون الصناعي غير الرسمي

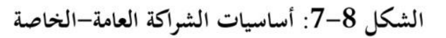
ومن بين السمات الأساسية لتحقيق شراكة ناجحة حيادية البرنامج، والنفوذ وقواعد تبادل البيانات وتحقيق الثقة وعضوية غير مفتوحة فضلا عن تشجيع المزايا والاستجابة.

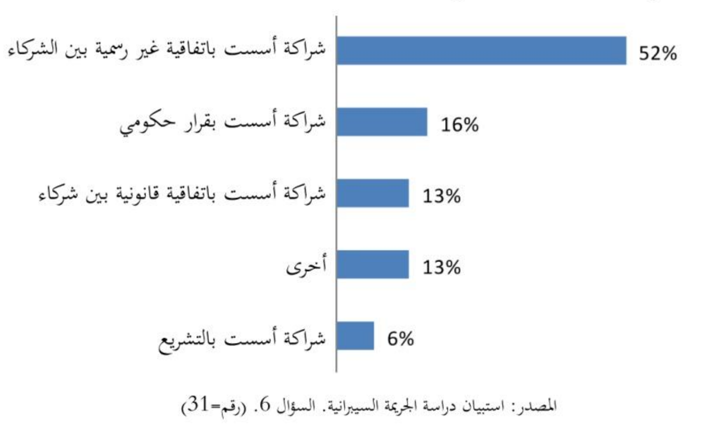
المصدر: 17 ECLR 1936, 31 Dec 2012

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 6.

من بينها الحاجة إلى استيعاب مشهد التهديدات المتطورة فضلا عن الحاجة إلى التعامل عن قرب مع مالكي القطاع الخاص ومشغلي البنية التحتية الرقمية.[1]

وأثناء جمع البيانات الخاصة بالدراسة، سُئلت منظمات القطاع الخاص عن وجود شراكات بين القطاع العام والخاص لمنع الجريمة السيبرانية ومكافحتها. وأشار أكثر من نصف الشركات المجيبة إلى مشاركتها في تلك المبادرات.[2] وعادة ما يتم الإبلاغ عن تلك الشراكات من خلال المنظمات والمؤسسات الأكاديمية ووزارات العدل وسلطات إنفاذ القانون ووزارات الأمن القومي ووزارات الاتصالات.[3] وأفادت الشركات بوجود الكثير من تجارب الشراكات الإيجابية، بما في ذلك إمكانية تبادل المعلومات حول مخاطر الجريمة السيبرانية والاتجاهات فضلا عن أفضل ممارسة لمنع الجريمة السيبرانية.[4] كما أشار عدد الشركات إلى التحديات المتمثلة في إقامة الشراكات والإبقاء عليها، حيث أكدت بعض الشركات على سبيل المثال على احتمالات وجود "*أهداف متباينة*" بين القطاع الخاص والسلطات الحكومية، كما أوضحت حاجة الشراكات بين القطاع العام والخاص لضمان أن *"تبادل المعلومات يسير في الاتجاهين"*.[5] وفي هذا الصدد، أكد عدد من منظمات القطاع الخاص متعددة على أنه يتعين أن تركز الشراكات على "*الحلول المشتركة*"، بما في ذلك التنظيم ومنع الجريمة.[6]


الشكل 8-7: أساسيات الشراكة العامة-الخاصة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 6. (رقم=31)

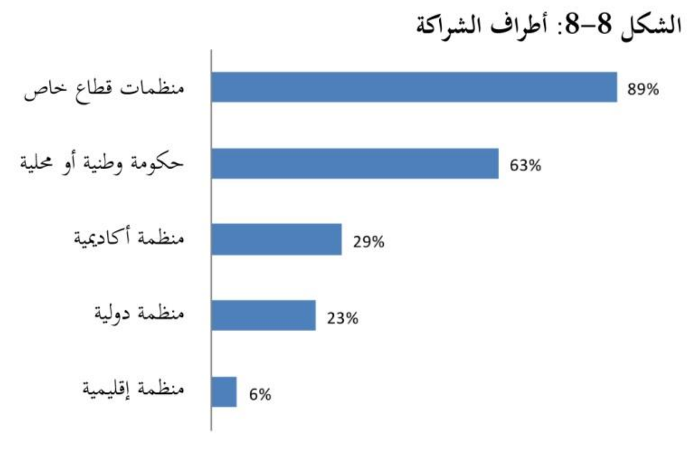
أشار أكثر من نصف البلدان المجيبة إلى أن الشراكات بين القطاع العام والخاص تقام من خلال اتفاق غير رسمي بين الشركاء، الأمر الذي يشير إلى الطبيعة غير الملزمة للعديد من تلك الترتيبات. وغالبا ما تنطوي الشراكات القائمة بموجب قرار حكومي على شركات تقدم بنية تحتية حيوية مثل المرافق والاتصالات.[7] وتعتمد الشراكات الأخرى المبلغ عنها على اتفاقيات قانونية بين الشركاء أو آليات أخرى، بما في ذلك مذكرات التفاهم وعضوية "مجموعة عمل". وكان التشريع الأساس الأقل إبلاغا (أكثر بقليل من 5 في المائة) لتنظيم ودعم أنشطة

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 6.
[2] استبيان دراسة الجريمة السيبرانية (القطاع الخاص). السؤال رقم 40-45.
[3] المرجع نفسه.
[4] المرجع نفسه.
[5] مقابلات بخصوص دراسة الجرائم السيبرانية (القطاع الخاص).
[6] المرجع نفسه.
[7] استبيان دراسة الجريمة السيبرانية. السؤال رقم 6.

الشراكة. ويتوافق هذا مع استخدام الشراكات بين القطاع العام والخاص باعتبارها استجابات ديناميكية قائمة على قضايا ذات اهتمام مشترك، والاحتياجات التشغيلية، فضلا عن ضرورة التصدي لتطور اتجاهات الجريمة السيبرانية.

وتماشيا مع المعلومات الواردة من منظمات القطاع الخاص، أفادت البلدان المجيبة بأن الشركات كانت من أبرز المشاركين في إقامة شراكات. وشمل 90 في المائة من الشراكات المبلغ عنها القطاع الخاص. بالإضافة إلى أن عددا من البلدان ذكرت المنظمات الأكاديمية والدولية والإقليمية.

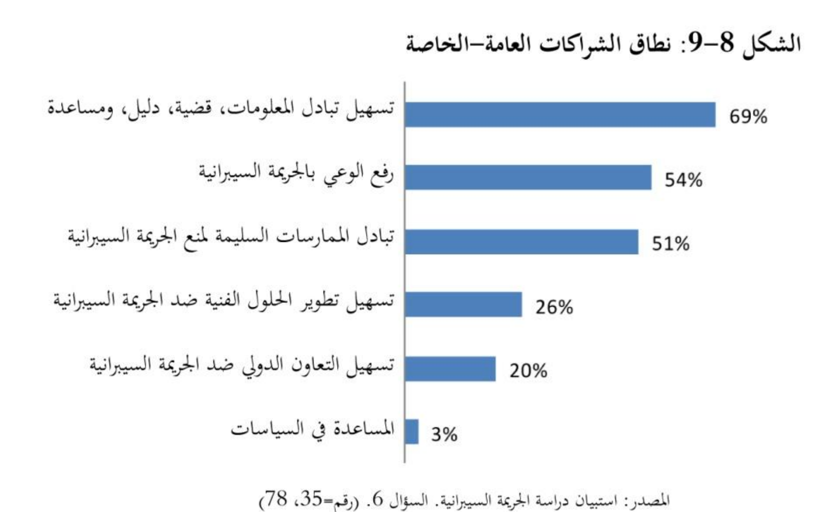
الشكل 8-8: أطراف الشراكة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 6. (رقم=35، 73)

تعكس نطاقات الشراكات بين القطاعين العام والخاص مجموعة من الأنشطة حيث أفادت بلدان بأن حوالي 70 في المائة من الشراكات التي وصفت بتضمنها على تبادل معلومات حول الجريمة السيبرانية. وأفادت البلدان على سبيل المثال أن الشراكات تستخدم من أجل "*تسهيل جمع الأدلة*" و "*التقرير التعاوني لبروتوكولات ومعايير العمل*"، بما في ذلك "*إقامة مراكز اتصال واحدة*".[1] وعند السؤال عن طبيعة تبادل المعلومات في تلك الشراكات، أفادت معظم البلدان بأنها تتعلق بالمعلومات الخاصة بمخاطر الجريمة السيبرانية فضلا عن الاتجاهات والمعلومات العامة حول أنواع قضايا الجريمة السيبرانية. ومع ذلك أشارت نصف الدول المجيبة إلى أن تبادل المعلومات اشتمل على معلومات خاصة بقضايا *محددة* للأفعال المنطوية على جرائم سيبرانية. وكما لوحظ في الفصل الخامس (إنفاذ القانون والتحقيقات)، فإنه يمكن للعلاقات الدائمة والفعالة بين سلطات إنفاذ القانون ومزوّدي الخدمات أن

الشكل 8-9: نطاق الشراكات العامة-الخاصة



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 6. (رقم=35، 78)

[1] استبيان دراسة الجريمة السيبرانية. السؤال رقم 6.

تساعد بصورة كبيرة في التحقيقات الفعّالة المتعلقة بالجريمة السيبرانية. وفي حال اشتملت تلك الترتيبات على تبادل بيانات شخصية، فمن المهم أن يتم تحقيق سيادة القانون والمعايير الدولية لحقوق الإنسان المتعلقة باليقين والضمانات القانونية بشأن منع الإساءة.[1]

وتشمل أنشطة الشراكة الأخرى المبلغ عنها أهداف تتعلق بزيادة الوعي بالجريمة السيبرانية، وتبادل الممارسات الجيدة لمنع الجريمة السيبرانية، وتسهيل تطوير الحلول الفنية ضد الجريمة السيبرانية.[2] فعلى سبيل المثال، تستشهد نصف البلدان المجيبة "*بتبادل طرائق الممارسة الجيدة*"، باعتبارها نشاط شراكة. وأشارت نسبة صغيرة من الدول الأعضاء المبلغة إلى أن الشراكات ساهمت في وضع السياسات. وفي ضوء اهتمام القطاع الخاص بالتطوير المشترك لسبل التصدي للجرائم السيبرانية، فإن هذا يمثل مجالا واحدا يمكن أن تتطوّر فيه الشراكات بين القطاع العام والخاص.

2-8 الوعي بالجريمة السيبرانية

الاستنتاجات الرئيسية

- تبين الاستقصاءات، بما في ذلك في البلدان النامية، أن معظم مستخدمي الإنترنت من الأفراد في الوقت الراهن يتخذون احتياطات أمنية أساسية
- يسلط جميع أصحاب المصلحة الضوء على الأهمية المستمرة لحملات رفع الوعي العام، بما في ذلك تلك التي تغطي التهديدات الناشئة، وتلك التي تستهدف جماهير محددة، مثل الأطفال
- تثقيف المستخدم يكون أكثر فعالية عندما يتم دمجه مع أنظمة تساعد المستخدمين على تحقيق أهدافهم بطريقة آمنة

زيادة الوعي

تسلط مبادئ الأمم المتحدة التوجيهية لمنع الجريمة الضوء على أهمية تثقيف الجمهور وتوعيته.[3] حيث تمثل زيادة الوعي العام بمخاطر الاحتيال والتدابير الوقائية التي يمكن اتخاذها استراتيجية هامة في الوقاية من أي نوع من أنواع الجريمة.[4] وبالإضافة إلى الحكومات، أثناء جمع المعلومات للدراسة، سلّطت منظمات القطاع الخاص أيضا الضوء على أهمية الوعي العام والمشترك فيما يتعلق بالجريمة السيبرانية. كما نوهت إحدى شركات الاتصالات

---

[1] أنظر الفصل الخامس، القسم 5.3، تدابير الخصوصية والتحقيق.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 6.

[3] مبادئ الأمم المتحدة التوجيهية في مجال منع الجريمة، 2002. قرار المجلس الاقتصادي والأمني 13/2002، المرفق. الفقرة 6 و25.

[4] أنظر على سبيل المثال، مكتب المم المتحدة المعني بالمخدرات والجريمة (UNDCP) 2010. دليل المبادئ التوجيهية في مجال الجريمة: Making them work.

الكبرى، على سبيل المثال، قائلة: "*يجب علينا تثقيف الناس بخصوص الأمن الأساسي. إن مالكي الأجهزة التي ليس لها أمن أساسي، أو رقع، أو تحديثات، يتركون أبوابهم مفتوحة على مصاريعها. ينبغي أن تكون الحملة جزءا من دور الحكومة كذلك، إن علينا إرسال رسائل بشكل مستمر عن أناس يحققون أفضل حماية لأنفسهم*".[1]

أشارت العديد من البلدان إلى مبادرات رفع الوعي. فقد أشارت إحدى البلدان المجيبة عن الاستبيان في الأمريكتين، على سبيل المثال، إلى أهمية "*الحملات الإعلانية في الإعلام، وتشغيل بوابات (ال7/24) الدردشة التفاعلية على الإنترنت، [و] تعزيز الشبكات والمواقع الاجتماعية.*"[2] كما نوه عدد من البلدان في أوروبا والأمريكتين أيضا إلى أنها وضعت استراتيجيات لرفع الوعي من خلال حملات لفترات محددة مثل "*شهر التوعية بالأمن السيبرانيي*" و"*يوم السلامة على الإنترنت*".

ذكرت إحدى البلدان علاوة على ذلك أنها "*أنشأت صفحة على فيس بوك، والتي تنشر... نصائح أمن سيبراني على الإنترنت ولها وصلات إلى بوابة للإبلا غ عن الشكاوى. هناك أيضا رقم هاتف الجرائم 1800- للإبلا غ عن حوادث الجريمة السيبرانية.*" كما أشارت إحدى البلدان في أوروبا إلى أن "*التدابير الرامية إلى تحسين الإبلا غ عن الجريمة السيبرانية قد تم تطويرها بشكل إضافي في 2007 مع إنشاء موقع متخصص على الإنترنت... يخدم هذا الموقع كمنصة معلوماتية ثنائية الاتجاه، حيث يمكن للشخص أن على معلومات بالأخطار التي تواجهه في فضاء الانترنت، ومن ناحية أخرى إرسال تقارير عن جرائم مرتكبة. ويتم توجيه التقارير بشكل مباشر إلى مسؤولي [الشرطة]... وفي الوقت الراهن، يتم استلام قرابة 150 تقريرا بشكل شهري عبر الموقع... من المتوقع عقب انطلاق الحملة للترويج للموقع أن يتزايد عدد الزيارات وعدد التقارير المقدّمة.*"[3] يلخص الجدول أدناه تفاصيل أربع حملات توعية تم ذكرها أثناء جمع المعلومات للدراسة.

ملامح حملات التوعية

1 مقابلة دراسة الجريمة السيبرانية (القطاع الخاص). حزيران/يونيو 2012.

2 المرجع نفسه.

3 المرجع نفسه.

	الحملة 1	الحملة 2	الحملة 3	الحملة 4
تم تمويلها وتنسيقها من قِبل	**حكومة أحد البلدان في شمال أوروبا**	**حكومة أحد البلدان في أوقيانوسيا**	**حكومة أحد البلدان في أمريكا الشمالية**	**حكومة أحد البلدان في أمريكا الجنوبية**
الملامح الرئيسية/المركزية				
الاستخدام الآمن، سرقة الهوية، الحيل	✓	✓	✓	✓
حماية الطفل، التنمر السيبراني	✓	✓	✓	
المحتوى الضار (العنف، المواد الإباحية، العنصرية)	ضمن حماية الطفل	✓		
القطاع الخاص – الحملات الموجهة، بما في ذلك القطاع المالي (التصيد، السلامة، الخ)				
التوعية بالإنترنت				
إعلانات الخدمة العامة، الأفلام	✓	حملات الخدمة العامة		✓
صفحات الويب المستهدفة	✓	✓	✓	
الألعاب التفاعلية		✓	التصفح الآمن عبر الإنترنت	
التنبيهات	آر إس إس، الفيسبوك، تويتر	خدمة البريد الإلكتروني المخصصة		
بيانات الضحية	✓			
بوابات تقرير مخصصة	بوابة تزييف العمل	بوابة الويب		بوابة الويب
المحادثات، الإحاطات، التوعية				
للمواطنين وعموم الجماهير	حدثت على طول الأسبوع سنويا، حملات إعلامية	أسبوع توعية سنويا	شهر التوعية بالأمن السيبراني سنويا	مؤتمر لمدة يومين
مجموعة خاصة من الطلاب والمعلمين والأخصائيين والأكاديميين وإنفاذ القانون، والقضاء	المؤتمرات والندوات والاجتماعات		شهر التوعية بالأمن السيبراني سنويا	التوعية المدرسية. التدريب الأساسي 6 أسابيع على الاستخدام الآمن لتكنولوجيا المعلومات للمتخصصين في المجال والطلاب

على الصعيد العالمي، تناول استعراض دولي بشأن التوعية بالأمن السيبراني والمبادرات التثقيفية في 2011، 68 من هذه الحملات، والتي استخدمت كلها الإنترنت كوسائل للاتصال. قدّم أكثر من ثلث الحملات منشورات، ونحو 30 في المائة ضمّن أيام أو أسابيع أو أشهر لرفع الوعي، بالإضافة إلى ندوات تدريبية وكتب إرشادية. كما استخدم الربع فيديوهات و ألعاب أو مسابقات. وقد تمت استضافة معظم الحملات من قبل وكالات حكومية، وإن جاءت غالبا كجزء من اتحاد يشمل شركاء من القطاع الخاص والمؤسسات غير الربحية.[1]

وبينما يتم تنظيم العديد من حملات التوعية على المستوى الوطني، يوجد أيضا عدد صغير من الأمثلة الإقليمية. نظام الإنذار وتبادل المعلومات الأوروبي، على سبيل المثال، أنشئ عام 2006. جمعت هذه الحملة معلومات ومواد تعليمية من أفرقة الاستجابة للطوارئ الحاسوبية ومجتمعات أمنية أخرى من بلدان في أوروبا. تمت ملائمة المواد بعد ذلك لمختلف فئات المواطنين والشركات الصغيرة ومتوسطة الحجم في كل بلد من البلدان المشاركة. وتم نشر المواد بواسطة وسائل الإعلام الاجتماعية، ومواقع الإنترنت، والقوائم البريدية. كما ركز نطاق واسع تجريبي على الوعي بالروبوتات، وسرقة الهوية، وتهديدات الهندسة الاجتماعية، وصلت إلى أكثر من 1,500 شخصا.[2]

أدارت شركات التكنولوجيا والجماعات غير الربحية أيضا حملات التوعية الخاصة بها. فحملة جوجل "من الجيد أن تعرف"، على سبيل المثال، نفّذت بحوالي 40 لغة منذ 2011. كما تعطي الإعلانات في الصحف والمجلات وعلى الإنترنت ووسائل النقل العام نصائح أمنية توضّح بعض خصائص الإنترنت الأساسية مثل ملفات تعريف الارتباط وعناوين بروتوكول الإنترنت.[3] عمل معهد سلامة الأسرة على الإنترنت أيضا مع شركات التكنولوجيا لتجميع مواد تثقيفية/تعليمية للوالدين، والأطفال، والمعلمين، في موقعهم "Platform for Good".[4] أدار كييفستار (Kyivstar)، مشغل اتصالات في أوروبا الشرقية، حملة "أخبر طفلك عن أمان الإنترنت" في نيسان/أبريل 2012، مع إعلانات في وسائل الإعلام المطبوعة، وعلى السيارات، وعلى الإنترنت، وأيضا مع متطوّعين يقدمون دورات معلوماتية في المدارس.[5] وأما بالنسبة للجمهور الأصغر سنا فقد أدارت ديسني

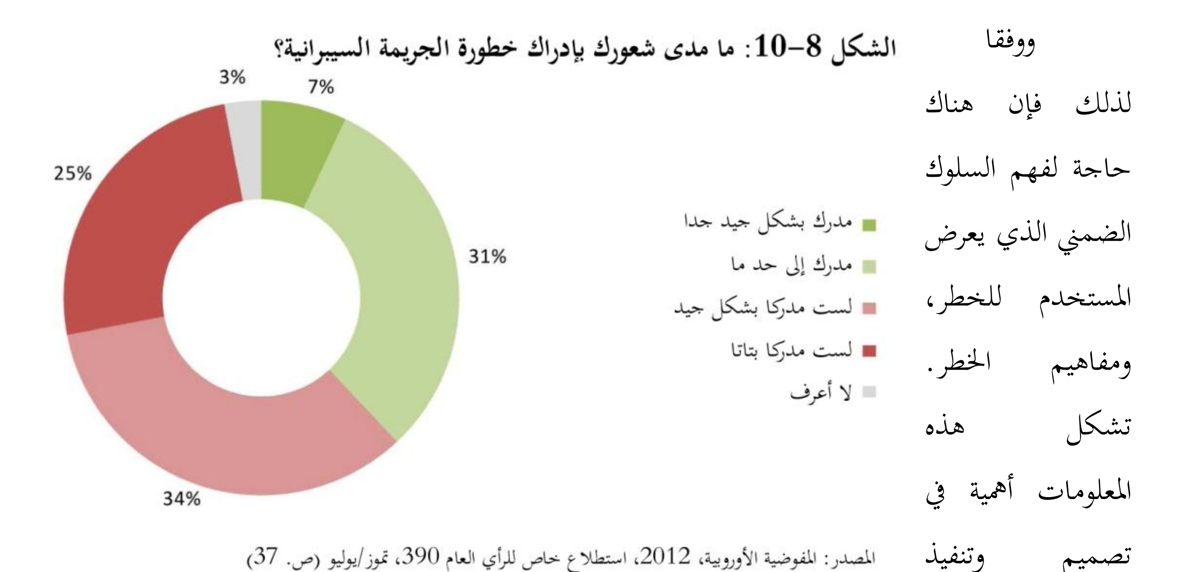
[1] أنظر: http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf
[2] Degenhardt, W. 2012. EISAS Large-Scale Pilot: Collaborative Awareness Raising for EU Citizens & SMEs, ENISA.
[3] أنظر: http://www.google.com/goodtoknow/
[4] أنظر: http://aplatformforgood.org/
[5] أنظر http://en.csrukraine.org.ua/?p=367

(Disney)، حملة سلامة تلفزيونية، ومن خلال موقع على الإنترنت، ومجلة، في 2012 هدفت للوصول إلى 100 من الأطفال والأهل في أوروبا، والشرق الأوسط، وأفريقيا.[1]

وعلى الرغم من العدد المتزايد لهذه الحملات، إلا أن عددا من البلدان نوّه إلى فكرة أن *"حملات التوعية العامة ستستغرق بعض الوقت لتبني ثقة العامة من أجل زيادة الإبلاغ عن الجريمة السيبرانية"*.[2] وأثبت الاستعراض الدولي 2011 للحملات كذلك أن القليل من الحملات تضمنت عنصر التقييم. كما سلّط الضوء أيضا على التحديات التي تواجه تطوير الحملات الملائمة والفعالة من حيث التكلفة، وأشار أيضا إلى أن تقديم المعلومات للمستخدمين دون أنشطة تدريب واكتساب مهارات إضافية يكون تأثيره محدودا على سلوكياتهم على الإنترنت. وختم الاستعراض بأن حملات بسيطة مرتكزة على مجموعات مستهدفة محددة يكون لها تأثير أكثر فعالية، على ما يبدو، من حيث التكلفة.[3]

وفقا لذلك فإن هناك حاجة لفهم السلوك الضمني الذي يعرض المستخدم للخطر، ومفاهيم الخطر. تشكل هذه المعلومات أهمية في تصميم وتنفيذ أنشطة التوعية بشأن الجريمة السيبرانية، فضلا عن منع الجريمة السيبرانية بشكل عام. يتناول القسم التالي من هذا الفصل المعلومات المبنية على السكان واستطلاعات الشركات في هذا المجال.

الشكل 8-10: ما مدى شعورك بإدراك خطورة الجريمة السيبرانية؟



المصدر: المفوضية الأوروبية، 2012، استطلاع خاص للرأي العام 390، تموز/يوليو (ص. 37)

[1] أنظر: http://www.guardian.co.uk/technology/appsblog/2012/jul/04/disney-club-penguin-child-safety

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 82.

[3] لمحة عامة عن التوعية الدولية بالأمن السيبراني والمبادرات التثقيفية. الاتصالات الأسترالية والسلطة الإعلامية. Galexia. 2011 .

فهم السلوك الذي يعرّض المستخدم للخطر

تظهر الاستطلاعات السكانية أن العديد من مستخدمي الإنترنت، على الأقل في البلدان الأكثر تقدما، "مدركون" لخطورة الجريمة السيبرانية. فقد أظهرت دراسة تم إجراؤها في بلدان أوروبية، على سبيل المثال، أن أكثر من 70 في المائة من الأشخاص قد سبق وأن سمع أو رأى معلومات عن الجريمة السيبرانية خلال العام الماضي، غالبا من التلفاز أو الصحف أو الإنترنت أو المذياع أو من الأصدقاء أو العائلة أو من الزملاء.[1] وتلقي المعلومات حول الجريمة السيبرانية، مع ذلك، لم يترجم بالضرورة إلى "شعور بالإدراك" للجريمة السيبرانية. فقد أفاد 7 في المائة فقط من المجيبين في نفس الاستطلاع بالشعور بإدراك "جيد جدا" بخصوص الجريمة السيبرانية. وما يزيد عن النصف أفاد بالشعور بعدم "الإدراك على الإطلاق"، أو بـ "عدم الإدراك بشكل جيد جدا".

تشير الاستطلاعات، إضافة إلى ذلك، إلى أن معظم مستخدمي الحاسوب، بما في ذلك في البلدان النامية، يأخذون الآن بعض احتياطات الأمن الأساسية. ففي استطلاع تم إجراؤه على أكثر من 13,000 من مستخدمي الإنترنت في 24 بلدا، أفاد ما يقرب من 90 في المائة من المجيبين بحذفهم لرسائل بريد إلكتروني مشبوهة واردة من أشخاص مجهولين. كما افاد حوالي 80 في المائة من المجيبين باستخدام برنامج أساسي لمكافحة الفيروسات على الأقل، وعدم فتح المرفقات أو الروابط في البريد الإلكتروني أو النصوص غير المرغوب فيها.[2] وأفاد نصف المجيبين فقط، مع ذلك، باستخدام إعدادات الخصوصية للشبكات الاجتماعية للسيطرة على تبادل المعلومات، إلا أن أكثر من 35 في المائة يقبلون طلبات صداقة من أشخاص مجهولين بالنسبة إليهم. يعكس هذا النمط إلى حد كبير استطلاعا دوليا آخر شمل ما يقرب من 4,000 من مستخدمي الإنترنت في ست دول في أمريكا الشمالية وأوروبا وخلص إلى أن 10 في المائة من مستخدمي البريد الإلكتروني قد نقر على روابط قد تكون محفوفة بالمخاطر في رسائل يشتبه أن تكون بريدا طفيليا، في حين أن أقل من 10 في المائة فقط قد فتح مرفقات في رسائل البريد الطفيلي.[3]

أما الاستطلاعات التي تم إجراؤها على الجيل الأصغر في بلدان أقل نموا فتظهر بشكل خاص مستويات مرتفعة من مخاطر الوقوع ضحية للجريمة السيبرانية. فقد أفاد استطلاع تم إجراؤه على أكثر من 25,000 طفل

---

[1] المفوضية الأوروبية. يوروبارومتر الخاصة 2012، 390.

[2] سيمانتك 2012. تقرير نورتن بشأن الجرائم السيبرانية لعام 2012.

[3] الفريق العامل المعني بمكافحة إساءة استعمال المراسلات (MAAWG)، الوعي بأمن البريد الإلكتروني وتقرير الاستخدام 2010. نيويورك: الشؤون العامة لأبسوس. تم ترجيح هذه الدراسة لتكون ممثلة لعدد مستخدمي الإنترنت في كل بلد.

في سن المدرسة في سبع دول في وسط وجنوب أمريكا بأن، من بين حوالي 45 في المائة من الأطفال الذين كان لديهم اتصال منزلي بالإنترنت، فقط حوالي 10 في المائة من اليافعين (10 إلى 18 عاما) أفاد بحيازته لبرنامج أمني مثبت (إن كان لتنقية الإنترنت أو مضاد فيروسات). و 20 في المائة من المجيبين لا يعرفون إن كان لديهم برنامج أمني مثبت أم لا.[1]

لا تنطبق المخاوف الأمنية وسلوك المخاطر على استخدام الحاسوب المكتبي فحسب. وكما تمت الإشارة في الفصل الأول (الموصولية العالمية)، فإن مزيدا من المستخدمين يدخلون إلى الإنترنت باستخدام جهاز محمول أكثر من الذين يدخلون من خلال خط ثابت عريض النطاق. وعلى الرغم من أن التهديدات الإلكترونية أصبحت سائدة على نحو متزايد بالنسبة للأجهزة المحمولة،[2] فإن المستخدمين ما يزالون يعتقدون أن الهواتف المحمولة والأجهزة اللوحية أكثر أمانا من الحاسوب المكتبي. كما توصل استطلاع تم إجراؤه على 11,000 من مستخدمي الإنترنت في أمريكا الشمالية وأمريكا اللاتينية وأوروبا والشرق الأوسط وآسيا وأفريقيا، على سبيل المثال، إلى أن 60 في المائة من المستخدمين يعتقدون أنه من "الآمن" أو "الآمن إلى حد ما" استخدام الهواتف الذكية دون تدابير وقاية إضافية، مقارنة بنحو 45 في المائة ممن يعتقدون ذلك بالنسبة للحواسيب المكتبية والمحمولة.[3]

الشكل 8-11: سلامة الجهاز المتصوّرة



المصدر: مختبر كاسبيرسكاي، 2012. التصوّر والمعرفة بتهديدات تكنولوجيا المعلومات (ص. 2)

حدود تثقيف المستخدم

تعد المشورة بشأن مخاطر الجريمة السيبرانية والتخفيف من آثارها بالنسبة للأفراد عنصرا هاما ضمن استراتيجية شاملة للحد من الجريمة السيبرانية. ومع ذلك فإن هناك حدودا بالنسبة للمدى المتوقع أن يتعلمه

---

[1] FundaciónTelefónica. 2008. La generacióninteractiva en Iboamérica: Niños y5 2 adolescentes ante laspantallas.

[2] أنظر على سبيل المثال، سيمانتيك Internet Security Threat Report.2012 . المجلد 17.

[3] معمل كاسبرسكاي. 2012. Perception and knowledge of IT threats: the consumer's point of view الصفحة رقم 2.

المستخدمون من الآليات الأمنية المعقدة، وتذكر كلمات السر الطويلة والمتنوعة لكل خدمة على الإنترنت يقومون بالدخول إليها، بالإضافة إلى اتخاذ الاحتياطات الأخرى التي غالبا ما تتدخل بشكل مباشر مع المهمة القائمة.[1]

ومما لا يثير الدهشة، أن العديد من المستخدمين لا يستطيعون أو لن يتبعوا المشورة الأمنية، وهو ما يشكل عبئا أكبر بكثير من النتائج الفردية المحتملة لفشل الأمن. فقد أفاد الباحثون في مجال الأمن، على سبيل المثال، إلى أنه *"في حالة استغل المستخدمون دقيقة واحدة من الوقت يوميا في قراءة عناوين المواقع لتجنب الخداع فإن التكلفة (من حيث وقت المستخدم) ستكون ضعفي حجم كافة خسائر الخداع"*.[2] كما يتطلّب فهم كافة الطرق المختلفة التي يمكن للموقع المنتحل من خلالها أن ينتحل صفة موقع معين سيحتاج استثمارا من الوقت والتثقيف، غالبا ما يكون معظم المستخدمين عقلانيين في رفضه.[3]

من المتوقع أن يكون تثقيف المستخدم أكثر فعالية إذا ما تم دمجه مع الأنظمة التي تساعد المستخدمين في تحقيق أهدافهم بطريقة آمنة. ينبغي أن يتطلب الأمر التأكيد المتعمّد عند محاولة المستخدمين القيام بأفعال من شأنها أن تضر بشكل خطير بأمن النظام الخاص بهم عن طريق تثبيت برامج مجهولة الأصل. ويجب أن تكون تكلفة التدابير الأمنية التي يتخذها المستخدم مناسبة بالنظر إلى المزايا التي تقدمها – فعلى سبيل المثال، قواعد كلمة مرور معقدة تتطلب استثمار المستخدم في تذكر كلمات مرور صعبة، ولكن يمكن بسهولة إبطالها من خلال مفتاح التسجيل أو هجمات الانتحال. إذا كانت تكلفة المستخدم أعلى من فائدته المباشرة، يكون للأفراد حافز قوي لتجاهل التدابير الأمنية.[4]

وبالتالي فإن، العمليات التنظيمية التي تعزز سلوك الوعي الأمني من قبل الموظفين والعملاء داخل مؤسسات وشركات القطاع الخاص حرجة – فعلى سبيل المثال، من خلال مساعدة المستخدمين في اختيار كلمة مرور آمنة بارزة للدخول في وقت مناسب، والتأكيد على أن كلمات المرور لن يتم طلبها على الإطلاق في مكالمة هاتفية أو بريد إلكتروني، أو عقب النقر على رابط في رسائل البريد الإلكتروني. وينبغي على الثقافة الاجتماعية والتنظيمية تجنب تبني الرأي الذي ينظر إلى السلوك الأمني "الرشيد" على أنه نوع من "جنون الارتياب" أو أنه أسلوب "متحذلق" ويشكل عائقا أمام الإنتاجية. لكن ينبغي على الثقافة التنظيمية بالأحرى مساعدة تشجيع

1 Sasse, M.A., Brostoff, S. and Weirich, D., 2001. Transforming the ‘weakest link’ - a human/computer interaction approach tousable and effective security. BT Technology Journal , 19(3):122-131.

2 Herley, C., 2009. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. New SecurityParadigms Workshop, Oxford.

3 المرجع نفسه.

4 المرجع نفسه.

السلوك الآمن ومكافئته.[1] يتناول الجزء التالي من هذا الفصل ممارسات الأمن السيبراني التي تبنتها مؤسسات القطاع الخاص.

3-8 منع الجريمة السيبرانية، القطاع الخاص والأوساط الأكاديمية

الاستنتاجات الرئيسية:

- أفاد مجيبو القطاع الخاص بوجود قدر من التوعية وإجراءات الأمن السيبراني. وقد أجرى ثلثا مجيبي القطاع الخاص تقييما لمخاطر الجريمة السيبرانية، حيث أفاد معظمهم باستخدام تقنية أمن سيبراني
- كما تم الإعراب عن القلق بأن الشركات الصغيرة والمتوسطة لم تتخذ الإجراءات الكافية لحماية النظم، أو لديها انطباع خاطئ بأنها لن تستهدَف
- وقد اتخذت بعض الشركات، من ضمنها مقدمو الخدمات وشركات التكنولوجيا، خطوات استباقية لمواجهة أفعال الجريمة السيبرانية، بما في ذلك استخدام الإجراءات القانونية
- يمكن لمقدمي خدمات الإنترنت ومقدمي خدمات الاستضافة الاضطلاع بدور أساسي في الحماية من الجريمة السيبرانية، إذ يجوز لهم الاحتفاظ بالسجلات التي يمكن استخدامها في التقصي عن الأنشطة الإجرامية ومساعدة العملاء في تحديد الحواسيب المعرضة للخطر ومنع بعض المحتويات غير المشروعة، مثل البريد الإلكتروني الطفيلي، ودعم بيئة الاتصالات الآمنة لعملائهم بشكل عام
- تمثل المؤسسات الأكاديمية شريكا مهما في منع الجريمة السيبرانية من خلال تطوير المعرفة وتبادلها ووضع التشريعات والسياسات، وتطوير التكنولوجيا والمعايير الفنية، وتقديم المساعدة الفنية، والتعاون مع سلطات إنفاذ القانون

يتناول هذا القسم ثلاثة جوانب من العلاقة بين القطاع الخاص والأوساط الأكاديمية والجريمة السيبرانية. (1) نُهُج الأمن السيبراني التي تتبناها منظمات القطاع الخاص، (2) الإجراءات التي يمكن لمقدمي خدمات الإنترنت اتخاذها لمنع الجريمة السيبرانية، (3) دور الأوساط الأكاديمية والمنظمات الحكومية الدولية في منع الجريمة السيبرانية.

1 Sasse, M.A., S Brostoff and D Weirich (2001) Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. BT Technology Journal , 19(3):122-131.

ممارسات الأمن السيبراني لمنظمات القطاع الخاص

طُرح أثناء جمع المعلومات المتعلقة بهذه الدراسة سؤال على منظمات القطاع الخاص عن ممارسات الأمن السيبراني التي تتبناها بهدف منع الوقوع ضحية للجريمة السيبرانية. وقُدمت هنا المعلومات الواردة من الشركات بالإشارة إلى المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي المتعلقة بأمن نظم المعلومات والشبكات.[1] وقد انعكست المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي في قرار الجمعية العامة بشأن إنشاء ثقافة عالمية للأمن السيبراني،[2] وكذلك في الصكوك الإقليمية.[3] وقد استخدمت غرفة التجارة الدولية هذه المبادئ التوجيهية لإصدار دليل مختصر عن "*ضمان أمن المعلومات للرؤساء التنفيذيين*" والذي يشير إلى أن "*لكل الأطراف دور تؤديه في الثقافة الأمنية، ولكن للمشروعات، مثل: المبتكر الرئيسي لتكنولوجيا المعلومات والاتصالات ومطورها ومقدمها، دور أوسع من الباقين*".[4] تؤكد المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية على ثلاث مجموعات من مبادئ الأمن السيبراني: (1) مبادئ "المؤسسة" و(2) المبادئ "الاجتماعية" و(3) ومبادئ "دورة حياة الأمن". وهي تمثل أساسا تنظيميا لنهج منع الجريمة السيبرانية التي أفادت بها شركات القطاع الخاص.

مبادئ المؤسسة – مبادئ "مؤسسة" للأمن السيبراني تتعلق بأهمية التوعية التنظيمية بالمخاطر، والمساءلة بناء على تلك التوعية، وعمليات التنسيق والتعلم للتعامل مع الحوادث.

أثناء جمع المعلومات المتعلقة بالدراسة، أكد مجيبو القطاع الخاص على أهمية اتباع نهج شامل للأمن في المؤسسة. وقد علق أحد الرؤساء التنفيذيين لدى إحدى الشركات قائلا: "*تستفسر الكثير من شركات التأمين عن بعض الأشياء تحديدا، مثل: هل لديك نظام التشفير، هل لديك جدران حماية، هل لديك برنامج مكافحة الفيروسات، ولكن ما نحاول معرفته حقا هو هل يشكل الأمن جزء لا يتجزأ من قرارات الأعمال التجارية التي تتخذها شركة مؤمنة – والتي من الصعب جدا الحكم فيها – لأن الكثير من الشركات ستتخذ الحد الأدنى الضروري من أجل حماية البيانات، لكنها لا تضع حماية البيانات على رأس أولوياتها......فعندما تنظر إلى الأمن والخصوصية باعتبارها وظائف منفصلة ومستقلة، مستقلة عن كل ما عداها مما تقوم به، فإن ذلك لا يتميز بالفاعلية.*"[5] وأضاف أحد مصنعي المعدات: "*الشركات بحاجة إلى برنامج إدارة المخاطر ووضع سياسات*

[1] توصية المجلس بشأن المبادئ التوجيهية لأمن نظم المعلومات والشبكات – نحو الثقافة الأمنية، منظمة التعاون الاقتصادي والتنمية، 25 يوليو 2012 – C(2002)131/FINAL.

[2] قرار الجمعية العامة للأمم المتحدة 57/ 239، المؤرخ 31 كانون الثاني/يناير 2003.

[3] أُنظر، على سبيل المثال مجلس أوروبا، قرار المجلس بشأن النهج الأوروبي نحو الثقافة الأمنية للشبكات والمعلومات 02/15723، المؤرخ 28 كانون الثاني/يناير 2003 واستراتيجيه منتدى التعاون الاقتصادي لدول آسيا والمحيط الهادئ لضمان الثقة في البيئات الإلكترونية وتأمينها واستدامتها، الذي أيده كبار المسئولين في تشرين الثاني/نوفمبر 2005.

[4] أنظر: http://intgovforum.org/Substantive_1st_IGF/Information.security%20assurance.pdf.

[5] مقابلة بخصوص دراسة الجريمة السيبرانية (القطاع الخاص).

وممارسات لتنظيم تلك المخاطر بشفافية...و كذلك القدرة على أداء المهمات آنيا يقلل من تكلفة وظيفة المراجعة." [1]

وقد ركز المجيبون على ضرورة القيادة على مستوى مجلس الإدارة؛ حيث أضاف أحد مصنعي المعدات قائلا: "*لا أعتقد أنه يوجد شخص قد صاغ متطلبات العناية الواجبة التي عليك اتباعها. فيما يتعلق بمجلس إدارتك عليك أن تعرف ما الذي يجب عليك العناية به، عليك أن تكون على علم ما إذا كانت شركتك تتبع الممارسات المناسبة التي تشكل العناية المفروضة في بلدك أم لا. [.....] ومن ثمّ فإنها لا تقوم بالرقابة المالية فسحب، بل تراجع نظم المعلومات للتأكد من امتثالها لأفضل الممارسات.*"[2] وأشارت شركة متوسطة الحجم لخدمات التكنولوجيا: "*معظم المؤسسات لديها عدد قليل من الأشخاص ممن هم على دراية تامة بالمخاطر، ومنهم من يكون على بينة من البيانات التي تجمعها المؤسسة. ولكن تكمن المشكلة في قلة عدد من هم على دراية بالأمرين معا.*"[3]

أفاد تقريبا كل المجيبين على استبيان الجريمة السيبرانية المتعلق بالقطاع الخاص بتعاملهم مع التوعية بالمخاطر من خلال تدريب الموظفين إضافة إلى السياسات والرقابة على الموظفين والعملاء ووصول الجهة الخارجية والاستخدام. وقد طورت هذه الإجراءات داخل الشركة على الصعيد العالمي لها، مع اختلاف تكلفة التطبيق وفقا لحجم المنظمة. وهي تشمل عناصر مثل: توزيع المعلومات حول آخر التهديدات وأوجه قصور الحلول الفنية.[4]

علق العديد من المجيبين عن الاستبيان بأن التدريب في العديد من الشركات لم يكن فعالا بما فيه الكفاية، على الرغم من أن إحدى شركات الخدمات الدولية نوّهت إلى أن "أسس ممارسة [أمن المعلومات والخصوصية] متأصلة على نحو متزايد."[5] في حين نوّه مدير أمن شركة تكنولوجيا متوسطة الحجم قائلا: "*تنتج معظم التحديات في الواقع بسبب أخطاءٍ بشريةٍ أو هندسةٍ اجتماعية. فالمستخدمون السذّج يمكن أن يكونوا هدفا للنجاح في الوصول إلى الشركة. وهذه إحدى التحديات التي نعمل عليها ... فإذا ما طبقت المؤسسة التدريب والسياسة الصحيحين فلن يحدث ذلك. ولذلك فالوقاية هي الأساس.*"[6] وافق على ذلك شركة اتصالات عالمية قائلة: "*إن التحدي الكبير الذي يواجهنا هو التوصل إلى التزام كافة الموظفين بالقواعد الأساسية للحجب والمعالجة.*"[7]

1 مقابلة بخصوص دراسة الجريمة السيبرانية (القطاع الخاص)

2 مقابلة بخصوص دراسة الجريمة السيبرانية (القطاع الخاص)

3 مقابلة بخصوص دراسة الجريمة السيبرانية (القطاع الخاص)

4 استبيان دراسة الجريمة السيبرانية. السؤال رقم 64-67

5مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

6مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

7مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

ورغم زيادة الوعي بالتهديد، إلا أن بعض البلدان المجيبة عن الاستبيان أشارت إلى أن ذلك لن يقود إلى تغيير السلوك بشكل فوري. فقد علّقت إحدى الشركات المصنّعة للمعدات قائلة: *"إنني أعتقد أن هناك الكثير من الإنتشار حول التهديد، لكن على الأشخاص أن يربطوا بين التهديد ومسؤولياتهم الشخصية ومسؤوليات الشركات"*.[1] وصرّحت منظمة خدمات الشركات قائلة: *"أعتقد أن هناك وعي حتمي بذلك لم يكن موجودا في السابق بين أهل الصناعة، ولكن العديد من الأشخاص ما يزالون على غير وعي بذلك. إنك إذا ما كنت مقْدِما على اختراق شركةٍ فليس من الضروري أن تدخل من الباب الأمامي. إنك ستدخل من خلال إرسال ملف PDF محور إلى رئيس الحساب عندما يكون رئيس الحساب أو نائبه في الخارج لقضاء العطلة وسوف يصاب من ملف PDF المذكور، ومن ثم فإنك ستمتلك الحاسوب المحمول الخاص بهم ثم تنتشر أكثر في الشبكة الخاصة بهم، وتدخل إلى حساباتهم وأنظمة الدفع. إنها مسألة التوعية بالأخطار والتحديث المستمر. ليس هناك حل سحري لأي من هذه."*[2]

انقسم المجيبون عن الاستبيان من القطاع الخاص بالتساوي تقريبا بين ممتلكي وحدة متخصصة مركزية واحدة تتعامل مع قضايا الجريمة السيبرانية، وممتلكي عدد من الوحدات المتخصصة (مثل الخاصة باتصال إنفاذ القانون وأمن تكنولوجيا المعلومات)، وممتلكي موظفين متخصصين في مناطق العمل المختلفة. ارتفع أعداد الموظفين المعنيين في الإجمالي بشكل بطيء مقارنة بحجم الشركة، متفاوتا مابين صفر إلى 38 (مع شخص واحد من غير مكان العمل من 120).

يتعامل الموظفون عادة مع حفظ أدلة البيانات وتحقيقات الإنترنت المتقدّمة، مع بعض المراقبة لتهديدات الجريمة السيبرانية والاتجاهات الناشئة، مباشرين التعاون في مجال إنفاذ القانون، ومتبعين نهج أمن نظام الحاسوب. يتم تدريبهم داخليّا بشكلٍ رئيسي، مع بعض التدريب الإضافي من قبل القطاع الخاص والأوساط الأكاديمية والمؤسسات غير الحكومية. وفي المقابل، يقدّم حوالي ثلث المجيبين عن الاستبيان التدريب بشأن هذه الموضوعات للمؤسسات الأخرى، بما في ذلك الشركات والمؤسسات الحكومية، والمنظمات الدولية والمؤسسات غير الحكومية في بعض الحالات.[3]

يعد الاستخدام المتزايد بسرعة لخدمات الحوسبة السحابية، واستخدام الموظفين لأجهزتهم الحاسوبية الخاصة (وخاصة الهواتف الذكية والأجهزة اللوحية) للدخول على أنظمة الشركة اثنين من التغييرات التكنولوجية الحديثة الرئيسية التي تؤثر على بيئة مخاطر أمن المعلومات. فقد أظهرت دراسة أجرتها إحدى شركات الأمن متعددة

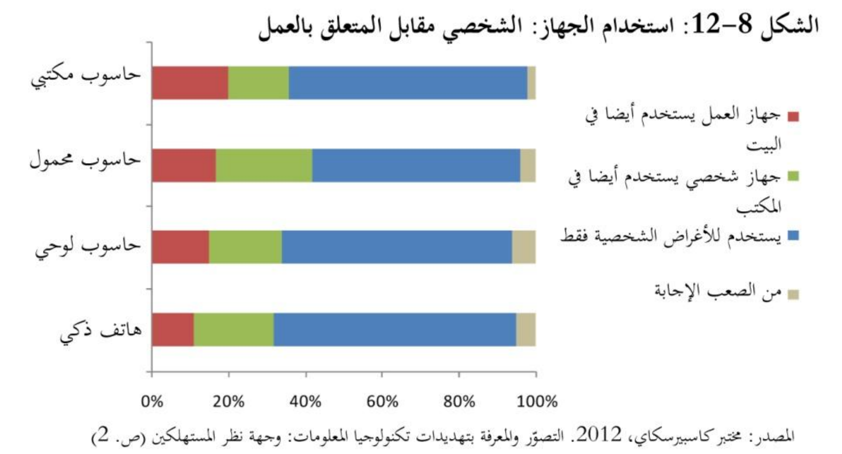
1مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

2مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

3استبيان دراسة الجريمة السيبرانية. (القطاع الخاص) السؤال رقم 68-73.

الجنسيات على 11,000 مستخدم للإنترنت في أمريكا اللاتينية وأمريكا الشمالية وأوروبا والشرق الأوسط وآسيا وأفريقيا، على سبيل المثال، أن حوالي 15 في المائة إلى 25 في المائة ممن تم إجراء الدراسة عليهم يستخدمون خدمات حاسوبية شخصية مختلفة في المكتب.[1]

الشكل 8–12: استخدام الجهاز: الشخصي مقابل المتعلق بالعمل



المصدر: مختبر كاسبيرسكاي، 2012. التصور والمعرفة بتهديدات تكنولوجيا المعلومات: وجهة نظر المستهلكين (ص. 2)

كما حدد المجيبون عن استبيان القطاع الخاص أيضا التأثير المتزايد لخدمات الحوسبة السحابية على الاعتبارات الأمنية. كما نوّهت إحدى شركات الاستشارات التكنولوجية المجيبين عن الاستبيان، على سبيل المثال: *"قد يكون استخدام السحابة بالنسبة للشركات الصغيرة أكثر أمانا من وجهة نظرٍ إلكترونية من محاولة قالقيام بذلك كل بنفسه باستعمال خادم شخصي. ليس هناك ما يكفي من خبراء الأمن السيبراني لتوفير واحد في كل شركة، لأن القيام بذلك سيكلف أموالا طائلة بدون شك. لذا فإن تركيز البيانات عند أمازون شيء منطقي جدا فيما يتعلق بالحماية وكذا فيما يخص الاستجابة. ومما لا شك فيه أن ذلك سيخلق فرصا يمكن استهدافها. وعلاوة على ذلك، فاختراق دفاعات مزود خدمات كبير شيء مثير حقا؛ أكثر من اختراق دفاعات دكان في الحي"*.[2] في حين سلّط مجيبون آخرون عن الاستبيان الضوء على قضية استخدام الموظفين لأجهزتهم الخاصة. فقد نوّهت إحدى شركات الاستشارات التكنولوجية قائلة: *"أعتقد أن تراكم الخطر ناتجٌ حقا عن جلب الجهاز الخاص. فالجميع يجلبون أجهزة عالية الكفاءة ثم يقومون بتوصيلها بالشبكات اللاسلكية، وبذلك يتنقلون بين وسائل الإعلام الاجتماعية والبريد الإلكتروني في العمل والحياة الخاصة. لذلك اعتقد أن التهديد الرئيسي يكمن في وجود قصور لدى الأشخاص في اعتبار المشكلة تمسهم هم أيضا بصفة شخصية."*[3]

المبادئ الاجتماعية – تتعلق المبادئ الاجتماعية لمنظمة التعاون الاقتصادي والتنمية (OECD) بالسلوك الأخلاقي والديمقراطي من قبل المشاركين في مجتمع المعلومات. ويشمل ذلك الوعي بتأثير الخروق الأمنية على

---

[1] Kaspersky Lab. 2012. Perception and knowledge of IT threats: the consumer's point of view.

[2] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

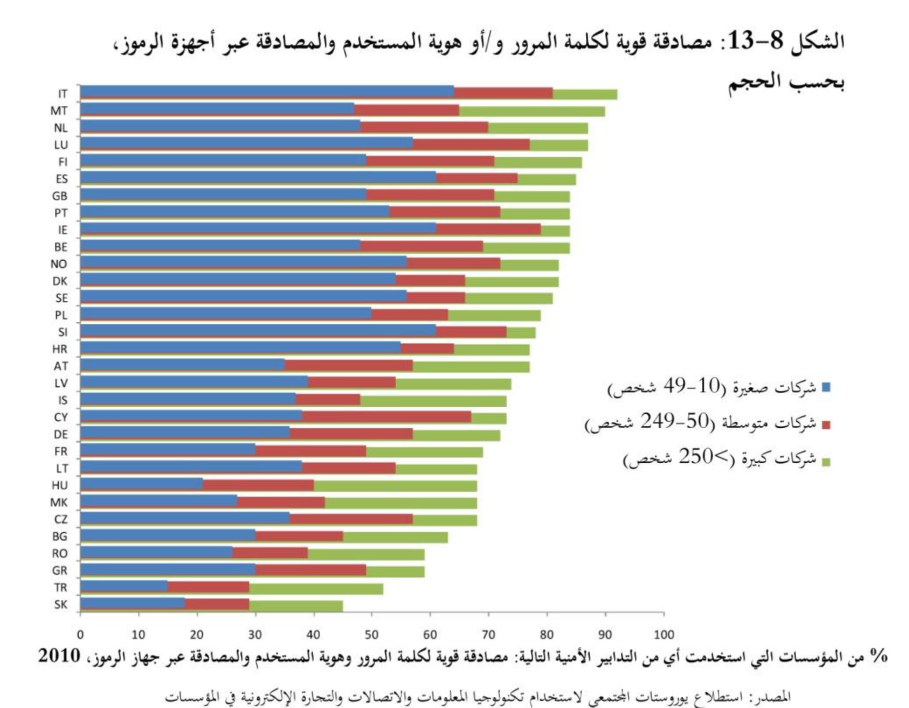
[3] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

الآخرين، وعلى التشريعات واللوائح ذات الصلة، وعلى كيفية مراعاة سلوك الموظف لقيم الشركة. كما يتعلق أيضا بتوافق الممارسات الأمنية مع القيم المجتمعية مثل حرية التعبير والخصوصية والانفتاح والشفافية.

كان المجيبون عن استبيان الدراسة من القطاع الخاص مسؤولين في المقام الأول عن القرارات الفنية والتجارية المتعلقة بالأمن والجريمة السيبرانية، بدلا من فرق المسؤولية القانونية أو الاجتماعية للشركات. علّق أحد المجيبين فقط فيما يخص المبادئ الاجتماعية، قائلا: "كانت فلسفة معظم الشركات في غضون السنوات القليلة الماضية أنه *"كلما زادت البيانات كلما كان ذلك أفضل" . إن عليك جمع أكبر قدر من البيانات يمكنك الحصول عليها لكي نستطيع بعد ذلك استخراج البيانات، واستخدام البيانات والقيام بالنمذجة المتوقعة، وما الضرر في جمع البيانات؟ مع القليل من التدبر في ماهية الضرر.*"[1] كما سلّط المجيب عن الاستبيان الضوء علاوة على ذلك على إمكانية تأثير هذا النوع من السلوك على تقييم المخاطر للشركات، في الوقت الذي اتجهت فيه بعض الشركات إلى التقليل من أهمية البيانات الشخصية التي تحتفظ بها والمخاطر المرتبطة بها التي قد تؤدي إليها.

مبادئ دورة حياة الأمن – ركز المجيبون من القطاع الخاص عن الاستبيان إلى حد كبير على مبادئ دورة حياة الأمن لمنظمة التعاون الاقتصادي والتنمية، الأكثر عملية في طبيعتها. هذه المبادئ تركز على تقييم المخاطر؛ وتصميم نظام للتخفيف من مخاطر محددة؛ وتطوير السياسات والعمليات والإجراءات لإدارة هذه النظم؛ بالإضافة إلى المراجعة المستمر التي تواكب تطور التكنولوجيا.

الشكل 8-13: مصادقة قوية لكلمة المرور و/أو هوية المستخدم والمصادقة عبر أجهزة الرموز، بحسب الحجم



% من المؤسسات التي استخدمت أي من التدابير الأمنية التالية: مصادقة قوية لكلمة المرور وهوية المستخدم والمصادقة عبر جهاز الرموز، 2010

المصدر: استطلاع يوروستات المجتمعي لاستخدام تكنولوجيا المعلومات والاتصالات والتجارة الإلكترونية في المؤسسات

تقدّم الاستطلاعات التي قامت بها شركات عالمية فكرة عن مدى تنفيذ

[1] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

هذه المبادئ. يظهر الشكل 8-13، على سبيل المثال، نسبة الشركات الأوروبية التي تستفيد من رموز الأجهزة لحماية التحقق من المستخدم.[1] يسلط الشكل الضوء على الاختلافات في مدى استفادة المؤسسات الصغيرة والمتوسطة والكبيرة من الممارسة الجيدة للأمن السيبراني – مع المؤسسات الأصغر حجما التي تستخدم باستمرارٍ ممارساتٍ أمنيةٍ أقل من التي تستخدمها المؤسسات المتوسطة والكبرى.

ذكر ثلثا المجيبين من القطاع الخاص عن استبيان الدراسة أن منظماتهم قد نفذت تقييم مخاطر الجريمة السيبرانية. في حين نوهت إحدى شركات الاستشارات التكنولوجية الكبرى قائلة: *"يطلب من القيادة التنفيذية للشركة، التحقق، مرتين في العام، من مخاطر أمن المعلومات ذات الأولوية، مقابل وجهة نظر قيادة منظمة أمن المعلومات. تشمل قائمة المخاطر قيد النظر الأعمال الإجرامية غير أنها لا تقتصر عليها"*. وصرحت شركةٌ مصنعةٌ للمعدات أن أساليب التقييم الخاصة بها تشمل *"المقابلات واختبارات الاختراق [و] واختبار المنتجات"*.[2]

أشار العديد من المجيبين إلى وجود تفاوت بين الشركات الكبيرة والصغيرة ومتوسطة الحجم في تقييم المخاطر. فقد صرحت إحدى شركات الاستشارات التكنولوجية متوسطة الحجم أن: *"[المؤسسات صغيرة ومتوسطة الحجم يعتريها شعور ب] "إننا لسنا ذوو أهمية؛ فهم لن يهاجموا أنظمتنا" وهذا غير صحيح. إنها مشتقة من "إننا لا نساوي الكثير؛ فهم لن يعتدوا علينا" وهو غير صحيح. إنها مشتقة من "إننا لا نعرف ما علينا القيام به" وهذا هو الصحيح."*[3] *كما أضافت شركة استشارات عالمية: "إن البنوك والشركات الكبرى مجهزة بشكل جيد نسبيّا للتعامل مع نشاط إجرامي اعتيادي. أما الأسواق متوسطة الحجم فليس لديها الكثير في مجال القدرة، إنهم يكافحون للرد، ولمعرفة ما يتأتى عليهم القيام بفعله."*[4] *وقد صرحت إحدى شركات الاستشارات التكنولوجية صغيرة الحجم قائلة: "لقد قدمنا الكثير من الندوات التثقيفية المجانية، وكان هناك حضور كبير لندواتنا عبر الإنترنيت من قبل الشركات صغيرة ومتوسطة الحجم. من المحتمل أن تأتي أيضا الشركات الكبرى للتثقيف المجاني، لكن الأغلبية ممن سيحضرون هي الشركات الصغرى ومتوسطة الحجم. إنها بدون شك في حاجة لهذه المعلومات"*.[5]

نوّه العديد من المجيبين إلى أن بعض الشركات الصغيرة ما تزال متوانية عن اتخاذ خطوات بسيطة لحماية أنظمتها. فقد علّقت إحدى شركات الخدمات الرئيسية: *"تفقد الشركات صغيرة ومتوسطة الحجم البيانات بسبب وسائل بسيطةٍ للغاية، وليست بسبب وسائل التكنولوجيا المتقدمة جدا (مثل شخص نسي تغيير كلمة المرور –*

---

[1] استطلاع المجتمع يوروستات بشأن استخدام تكنولوجيا المعلومات والاتصالات والتجارة الإلكترونية في الشركات.

[2] استبيان دراسة الجريمة السيبرانية(القطاع الخاص)السؤال رقم 49.

[3] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

[4] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

[5] المرجع نفسه.

وأشياء من هذا القبيل)... ربما لا تؤمّن معظم الشركات البيانات الخاصة بها في وقت الراحة، وإنما فقط في وقت النقل." [1] وأضافت شركة استشارات تكنولوجيا قائلة: *"إن النصائح التي نقدمها للناس في المقام الأول أشياء مثل: تأكد من أن نظامك مصحح تماما حتى الآن؛ تأكد من أنك لديك أجهزة/برامج مكافحة الفيروسات محدّثة بانتظام؛ إذا كنت في استغناء عن منتجات جافا وأدوبي فقم بحذفها؛ امتلك حاسوبا قائما بذاته تقوم باستخدامه في المعاملات المصرفية عبر الإنترنت فحسب. ولكن لن تستطيع مجابهة الدخول الفوري."*[2] ولكن الأمر لم يسلم حتى في الشركات الكبرى، فقد ذكر مقدم لخدمات التكنولوجيا العالمية أن *"الكثير من الاختراقات كان ومزال من الممكن الوقاية منها — وكلها تتعلق بإعدادات أساسية."* [3]

نوّه معظم مجيبي القطاع الخاص إلى استخدام الحلول التقنية لمنع الجريمة السيبرانية، مثل جدران الحماية والحفاظ على الأدلة الرقمية والقيود التي تفرض على اتصالات عنوان بروتوكول إنترنت محدد. كما يستخدم الكثيرون أيضا تعريف أنماط معينة من المحتوى، وتدابير لمنع انتهاك حقوق الطبع والنشر/العلامة التجارية، فك تشفير مواد مشفّرة، وتدابير لمكافحة إساءة استخدام الحاسوب. شملت العناصر الرئيسية لهذه الحلول الإشراف على النظام ومراقبته، وكشف التسلل وبرامج مكافحة الفيروسات. كما تم التنويه إلى الأنظمة بغية تطويرها في الغالب من قبل القطاع الخاص، مع بعض التطوير الداخلي، وامتلاك ميزانية تتبيث سنوية كبيرة، خصوصا بالنسبة للشركات متعددة الجنسيات المجيبة.[4]

اختلف المجيبون بشأن التهديد الذي يشكله "المطلعون" (الموظفون أو الأشخاص الآخرين المخوّلون للوصول إلى النظام). أشارت اثنتان من الشركات متعددة الجنسيات إلى مدى الضخامة التي وصل إليها عدد مجموعة "المطلعين" المحتملين في داخل مؤسساتهم: حيث ذكرت إحداهن عدد *"300,000 موظف حول العالم، بالإضافة إلى المقاولين"* .[5] في حين ذكرت الأخرى عدد *"200,000 موظف و 50,000-60,000 محاسب أو موظفي العقود بالنيابة عن الشركة"* .[6] عبر أحد المصنعين عن قلقه إزاء *"التواطؤ بين المطلعين والمجرمين الخارجيين [مع] مطلعين يعطّلون النظم الداخلية وعمليات التصنيع.*[7] ولكن كانت إحدى شركات الاستشارات الأمنية أقل قلقا، بخصوص الشركات المتطورة على الأقل: *"نعم، هناك أحيانا بعض المطلعين، لكننا لا نطلعهم على الكثير.*

---

[1] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

[2] المرجع نفسه.

[3] المرجع نفسه.

[4] استبيان دراسة الجريمة السيبرانية (القطاع الخاص)السؤال رقم 60-63.

[5] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

[6] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

[7] مقابلة دراسة بشأن الجريمة السيبرانية (القطاع الخاص).

إنما ينتج معظم الضرر من أطرافٍ خارجية. وبالتأكيد فإن البنوك مجزأة للغاية؛ حتى إن وجد فيها مطلعون فإن الضرر الذي قد يلحِقه هذا المطلع محدود للغاية." [1]

يعد تقييم السياسات والإجراءات الأمنية واستعراضها جزءا رئيسا من مبادئ دورة الحياة الأمنية التي تضعها منظمة التعاون والتنمية الاقتصادية. وقد أشار عدد من البلدان المجيبة إلى أهمية الرصد في الوقت الحقيقي للحوادث التي تمس بالأمن. وقد علقت شركة استشارات عالمية: "*نحتاج إلى آليات قابلة للتنفيذ والمشاركة في الوقت الحقيقي. وهذه مشكلة معقدة؛ حيث يجب تصنيف المعلومات وإعطاؤها الأولوية وتحديدها عندما تتسم الحوادث بالخطورة، ويجب على الجميع التحدث باللغة ذاتها حتى وإن لم يتشاركوا في الأهداف ذاتها، ومجددا القابلية للتنفيذ في الوقت الحالي.*" [2] وقد أضافت شركة استشارات عالمية أخرى: "*بمجرد معرفتهم، يستجيبون على النحو الصحيح. ولكن ما نواجهه الآن هو أن عددا من الشركات لا تصلح بما يكفي للكشف ...... 12 دقيقة، وليس 12 شهرا.*" [3]

دعوى Golden Eye v Telefónica

رفعت شركة إنتاج سينمائي ومالكو حقوق تأليف ونشر أفلام إباحية دعوى عام 2011 للحصول على أسماء وعناوين ما يقرب من 10,000 من عملاء مزود خدمة إنترنت قد ادعت مخالفتهم لحقوق التأليف والنشر باستخدام BitTorrent لمشاركة الملفات. ولم تسمح المحكمة العليا في أحد بلدان شمال أوروبا بهذا الإجراء إلا لواحد من المشتكين فقط، وقد علقت أن ما هو أبعد من ذلك "سوف يعادل فرض العقوبة على بيع المدعى عليهم المعنيين لحقوقهم في الخصوصية وحماية البيانات لمن يقدم أعلى سعر" كما أعربت المحكمة عن قلقها بأن طبيعة الأفلام محل التقاضي يمكن أن تجبر العملاء الأبرياء على سداد "رسوم تسوية" مرتفعة و"غير مدعومة".

وقد وضعت المحكمة عددا من الشروط على الخطاب الذي يمكن إرساله للمنتهكين المزعومين؛ نظرا "للأثر ... على العملاء العاديين الذين يحتمل أن ليس لهم الإمكانيات التي تخولهم الحصول على الاستشارة القانونية المتخصصة، والذين يحتمل عدم ارتكابهم للأفعال التي يتهمون بالضلوع فيها، وكذلك لما قد يصيبهم من الشعور بالخزي و/أو الأذى النفسي بسبب اتهامهم بالتورط في مشاركة ملفات تتضمن مواد إباحية."

وفي ظل هذه الضمانات، أيدت محكمة الاستئناف الحكم المستأنف من طرف إثني عشر آخرين من المدعين. كما أمرت محكمة الاستئناف مزود خدمات الإنترنت بالإفصاح عن تفاصيل بيانات جميع العملاء الضالعين، وذلك للتمكين من اتخاذ المزيد من الإجراءات ضد كل واحد منهم."

سلط عدد من المجيبين من القطاع الخاص، برغم ذلك، الضوء على أنه يمكن للشركات القيام بما هو أكثر من ذلك لحماية نفسها من التهديدات السيبرانية. وقد قال مزود خدمات تكنولوجيا عالمي: *"تتراوح*

---

[1] المرجع نفسه.

[2] مقابلة بخصوص دراسة الجرائم السيبرانية. (القطاع الخاص)

[3] المرجع نفسه

التهديدات/الاتجاهات ما بين البسيط والأكثر تعقيدا. ويكمن الأساس في التعرف على الشبكة والتحكم فيها من حيث إعدادات التطبيقات وتطوير نظام استخبارات معقد..." [1] بينما أشار مزود خدمات تكنولوجيا عالمي آخر: *"لا يستطيع معظم العملاء إعطاء الأولوية للأمن على مدار الساعة (رصد المعلومات/الأمن)"*. [2] وقد اقترحت شركة استشارات عالمية *أن "يجب تنفيذ بعض المهام الاستخباراتية الأمنية خارجيا، للعمل تقريبا كمركز لتبادل المعلومات أو القيام بالعمليات الخاصة باتخاذ القرارات الأمنية، بدلا من قيام كل منظمة كبرى بتشغيل مركز أمني عالمي لتجميع البيانات الاستخبارية الخاص بها"*. [3]

وبالإضافة إلى التركيز *داخليا* على وضعها الأمني السيبراني، نهجت بعض شركات التكنولوجيا العالمي نهجا خارجيا استباقيا للتحقيق في الهجمات الإلكترونية التي تهدد ثقة العملاء في نظمها وإيقافها. ويمكن لهذه المبادرات في حال تنفيذها بما يتوافق مع القوانين ذات الصلة أن تشكل دعما للأعمال التي تقوم بها هيئات إنفاذ القانون، مما يترتب عنه دعاية إيجابية ورفع الروح المعنوية للموظفين.

فمن الملاحظ؛ أن بعضا من هذه السِلْسِلَة الأطول من الإجراءات القانونية المتواصلة تتَعَلّق برسائل البريد الإلكتروني الطفيلي، إلى جانب بعض المراسلات الأخرى غير المرغوب فيها، مثل الرسائل الفورية. وفي عام 1997، أقام أحد أكبر مزودي خدمات الإنترنت بأمريكا الشمالية العشرات من الدعاوى القضائية ضد مرسلي البريد الإلكتروني التطفلي، وتمثلت الادّعاءات في التعدي على أملاك منقولة، والإثراء غير المشروع، وإساءة الائتمان، فضلا عن انتهاكات قوانين الجرائم الحاسوبية[4]. وفِيمَا بَعْد؛ ووفقا لقوانين مكافحة البريد الإلكتروني الطفيلي والتآمر[5] اتخذت مجموعة من أحد مزودي خدمات الإنترنت في أمريكا الشمالية والتي شكلت في عام 2003 تحالفا لمكافحة البريد الإلكتروني الطفيلي إجراءات قانونية ضد مجموعة من المتهمين المسؤولين عن إرسال مئات الآلاف من الرسائل غير المرغوب فيها لعملائهم.

ولقد اتخذت مؤخرا إحدى شركات البرمجيات العالمية عددا من الإجراءات القانونية مركزة على شبكات الروبوت، وذلك من خلال أسلوبين متداخلين رئيسيين: التَمَكّن من فرض السيطرة والتحكم في الآليات المستخدمة لتوجيه الآلات في إحدى شبكات الروبوت، بالإضافة إلى مصادرة الآلات التي تتضمن أدلة مفيدة تتعلق بالإجراءات الجنائية. وفي إحدى الدعاوى القضائية التي رفعت مؤخرا ضد شبكة الروبوت (Nitol)، أقامت الشركة دعوى قضائية لتتولى السيطرة على 70,000 من النطاقات الفرعية الخبيثة. هذا، وقد وافقت الشركة على

---

[1] مقابلة بخصوص دراسة الجرائم السيبرانية. (القطاع الخاص)

[2] مقابلة بخصوص دراسة الجرائم السيبرانية. (القطاع الخاص)

[3] المرجع نفسه

[4] Sorkin, D.E., 2001.Technical and Legal Approaches to Unsolicited Electronic Mail. *University of San Francisco Law Review,* 35(2):359-260.

[5] McGuire, D., 2004. AOL, E-Mail Companies Sue Spammers. *Washington Post*, 28 October.

إجراء تسوية لإعادة توجيه اتصالات النطاقات الفرعية الخبيثة المحددة الموجودة والمستقبلية لأحد الأجهزة التي يديرها فريق مواجهة الطوارئ الحاسوبية بشرق آسيا، مما خَفّض من قدرة مشغل شبكة الروبوت على التحكم في الأجهزة من أجل الوصول إلى هذه النطاقات، كما أتاح الفرصة لإخطار هؤلاء المستخدمين ومزودي خدمات الإنترنت التابعين لهم بتعرض أجهزتهم للخطر.

هذا، وقامت الشركة في الأيام الستة عشرة بعد سيطرتها على النطاقات الفرعية الخبيثة بحظر الاتصالات من 7.65 مليون عنوان فريد من عناوين بروتوكول الإنترنت، كما قدم المشغل والشركة جميع الأدلة التي تم جمعها أثناء التحقيق إلى فريق مواجهة الطوارئ الحاسوبية بشرق آسيا للمساعدة على تحديد مشغلي النطاقات الفرعية الأصليين. وقد تشاركت كل من الأفرقة الوطنية لمواجهة الطواري الحاسوبية، مع (Shadow Server Foundation)، البيانات المتعلقة بالأجهزة المصابة. وجدير بالذكر أن الشركة قد اتخذت مُسَبَّقا إجراءات مماثلة ضد شبكات الروبوت؛ Waledac، Rustock، Kelihos، وZeus[1] .

وقد اتخذت الشركة في الدعوى التي أقامتها ضد شبكة الروبرت (Zeus) إجراءات تدخُّل بشكل أكثر. وبعد الحصول على مذكرة إحضار من أحد قضاة المحكمة الفيدرالية، قام محامو الشركة والموظفون الفنيون بحجز الأدلة وتعطيل خوادم الاستضافة في ولايتي بنسلفانيا وإيلينوي التي تتحكم في شبكة الروبوت (Zeus). ومن ناحية أخرى؛ فرضت الشركة سيطرتها على 800 نطاق مستخدم لترتيب الحواسيب المصابة، حيث تهدف هذه الإجراءات إلى تعطيل عمل شبكات الروبوت، نظرا لعدم إمكانية تجميد نشاطها بالكامل.[2]

وتتمثل استراتيجية قانونية ثالثة استخدمتها الشركة في اتخاذ إجراءات ضد مُسْتَحْدِثي الشِفْرَات الخبيثة بُغْيَة منعهم من إنتاج روبوتات وشِفْرَات ضارة جديدة متى قد تم تجميد أنشطتهم السابقة. ففي عام 2012، أقامت الشركة دعوى قضائية معدلة في إحدى محاكم الولاية في أمريكا الشمالية ضد أحد المبرمجين في أوروبا الشرقية، والذي يبدو أنه اضطلع باستخدام الشفرة الخاصة بالشركة في شبكة الروبوت (Kelihos)، بيد أن المبرمج المعني قد أبدى استعداده للدخول في اتفاقية تسوية سرية.[3]

وعلى نحو مماثل، في عام 2012، اتخذت إحدى شركات مواقع التواصل الاجتماعي إجراءات ضد مزودي أدوات إرسال الرسائل الإلكترونية الطفيلية،[4] حيث أقامت دعوى قضائية ضد "خمسة من أكثر مزودي

---

[1] Microsoft Reaches Settlement with Defendants in Nitol Case. 2012. *The Official Microsoft Blog*, 2 October, available at: http://blogs.technet.com/b/microsoft_blog/archive/2012/10/02/microsoft-reaches-settlement-with-defendants-in-nitol-case.aspx

[2] Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets. 2012. *The Official Microsoft Blog*, 25 March, available at: http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx

[3] Microsoft Reaches Settlement with Second Kelihos Defendant. 2012. *The Official Microsoft Blog*, 19 October, available at: http://blogs.technet.com/b/microsoft_blog/archive/2012/10/19/microsoft-reaches-settlement-with-second-kelihos-defendant.aspx

[4] Shutting down spammers. 2012. *Twitter Blog*, 5 April, available at: http://blog.twitter.com/2012/04/shutting-down-spammers.html

الأدوات ومرسلي الرسائل الإلكترونية الطفيلية الأكثر شراسة"، وأدعت الشركة في دعواها أنهم قاموا بانتهاكات لشروط الخدمة وتحريض مستخدمي الأدوات على ارتكاب مخالفات. وقد سعت الشركة للحصول على أمر قضائي بمنع الجناة من إنتاج هذه البرمجيات وتوفيرها، كما طالبت بمبلغ 700,000 دولار أمريكي على الأقل كتعويض عن الأضرار التي لحقت بها.[1] وفي هذا الشأن أيضا؛ اتخذ اثنان من مزودي خدمات الإنترنت إجراءات قانونية ضد المعلنين الذين أساءوا استخدام خدماتهم. وقد حصلت إحدى شركات محركات البحث الكبرى –على سبيل المثال – على أمر نهائي ضد إحدى الشركات التي قد أعلنت عن مخططات لتحويل الأموال بشكل احْتِيَالِيّ،[2] كما قاضت المدعى عليهم الذين قاموا عن عمد بانتهاك شروط الخدمة التي فرضتها.[3] وعلى نحو مماثل، أقامت إحدى شركات شبكات التواصل الاجتماعي الكبرى دعوى قضائية ضد إحدى الشركات التي قامت بتصميم صفحات ووضع وروابط إلكترونية لخداع المستخدمين ليقدموا معلومات شخصية، ويسجلوا اشتراكهم في خدمة ذات رسوم اشتراك باهظة الثمن، وليضغطوا على كلمة "أعجبني" في أحد صفحات المواقع الإلكترونية، ومن ثم مشاركتهم مع أصدقائهم.[4] بيد أن المدعى عليه أجرى تسوية مع الشركة.

وقد جمع عدد من شركات أمن الإنترنت مزيدا من البيانات التفصيلية عن انتشار البرمجيات وشبكات الروبوت الضارة، والتي قد نشرت في تقارير منتظمة شاركت فيها نظيراتها من الشركات وهيئات إنفاذ القانون. وتنشر العديد من الشركات تقارير ربع سنوية تحمل التهديدات الموجهة، وتحتوي على بيانات بشأن مستويات الأجهزة المصابة (بما فيها أجهزة الهاتف الجوال) واختراقات لقواعد البيانات وأعمال هجومية مثل التصيد والاحتيال وبعض أنشطة الجريمة السيبرانية، مثل طلب الفدية، وأدوات برمجيات الجريمة.[5] كما نشرت إحدى شركات الأمن في أوروبا الشرقية بيانات مجمعة عن مجموعات وأشخاص متورطين في جرائم سيبرانية بالإقليم،[6] بينما نشرت مؤخرا شركة أمن أخرى تقارير تتعلق بالمقارنة بين الملفات التعريفية للمهاجمين في شرق آسيا وأوروبا الشرقية.[7] هذا، وتشارك العديد من شركات الاتصالات السلكية واللاسلكية البيانات المعنية بحركة الأنماط

[1] *Twitter Inc. v. Skootle Corporation*. 2012. US District Court, Northern District of California, case no. CV 12-01721, 5 April.

[2] مكافحة الاحتيال عبر الإنترنت: taking 'Google Money' scammers to court. 2009. *Google Official Blog*, 8 December, available at:http://googleblog.blogspot.co.uk/2009/12/fighting-fraud-online-taking-google.html

[3] Taking rogue pharmacies to court. 2010. *Google Official Blog*, 22 September, available at:http://googleblog.blogspot.co.uk/2010/09/taking-rogue-pharmacies-to-court.html

[4] Facebook, Washington State AG Target Clickjackers. 2012. *Facebook Security Notes*, 26 January, available at: http://www.facebook.com/notes/facebook-security/facebook-washington-state-ag-target-clickjackers/10150494427000766

[5] انظر على سبيل المثال، *McAfee Threats Report: Third Quarter 2012*, available at: http://www.mcafee.com/us/resources/reports/rpquarterly-threat-q3-2012.pdf

[6] Group-IB. 2012.*State and Trends of the 'Russian' Digital Crime Market 2011*, available at: http://group-ib.com/images/media/GroupIB_Report_2011_ENG.pdf

[7] Trend Micro. 2012. *Peter the Great Versus Sun Tzu*, available at: http://www.trendmicro.com/cloud-content/us/pdfs/securityintelligence/spotlight-articles/op_kellermann_peter-the-great-vs-sun-tzu.pdf

والهجمات التي أمكن رصدها على شبكاتهم. وتبرز إحدى هذه المراصد، على سبيل المثال، خريطة بالوقت الفعلي للتهديدات العالمية مع ملخصات يومية عن الأحداث الهامة.[1]

ومن بين الظواهر الحديثة؛ قيام الشركات بدراسة استخدام المعلومات الاستخباراتية كرد على مثل هذه الهجمات، ويساعد العديد من كيانات القطاع الخاص الشركات من خلال إمدادها بلمحات مختصرة عن الخصوم وعن الدوافع التي تقف خلف قيامهم بهذه الهجومات. وتمكِّن هذه المعلومات من القيام بالدفاع التقني بشكل أفضل، والمواءمة الدقيقة للإجراءات القانونية، وكشف التَدْلِيس (مثل وضع معلومات خاطئة عن الشركة على الشبكة الخاصة بها) والهجمات كثيفة الاستخدام للموارد.[2] وقد درست بعض الشركات مسألة "إعادة الاختراق" ضد المهاجمين، بيد أن ذلك فِي الوَقْتِ الْحَالِي لم يتضح مدى مشروعيته أو ما إذا كان ملائما تقنيا.[3]

وتعتبر الصورة التي أشار إليها المجيبون من القطاع الخاص بشأن منع الجريمة السيبرانية مختلطة بشكل إجمالي. فلدى الشركات الكبرى، وخاصة في قطاع الخدمات المالية، استراتيجيات مُطَوّرة لمنع الجريمة السيبرانية، بما في ذلك استخدام بعض أساليب التكنولوجيا الأمنية، مثل رموز توثيق الأجهزة. وتضطلع شركات الأمن برصد ونشر تقارير منتظمة بشكل فعال بشأن ظُهُور تهديدات جديدة، فِيمَا اتخذت بعض شركات التكنولوجيا الكبرى إجراءات قانونية استباقية لتجميد نشاط شبكات الروبوت والمتطفلين والمحتالين، ومع ذلك؛ تعتبر الشركات الصغيرة في موقف غير جيد، إذ أن بعضها لا يتخذ الاحتياطات الأساسية أو ليس لديه أي صورة واقعية عن المخاطر الأمنية.

منع الجريمة السيبرانية من خلال مقدمي خدمة الإنترنت والاستضافة

يعتبر مزوّدو خدمة الإنترنت ومزودو الاستضافة على نحو فريد ضمن البنية التحتية للإنترنت. وكما هو موضح في الفصل الأول (الموصولية العالمية)، يمتلك مزودو الخدمة أليافا ضوئية عالية السعة أو يستأجرونها؛ وكذلك أسلاك نقل، فضلا عن البنية التحتية الأساسية الأخرى مثل الخوادم، ومفاتيح التبديل، والموجهات، وخلايا لاسِلْكِيّ (في حالة مشغلي الشبكات المحمولة) التي تتيح استضافة المحتوى وتقديمه، فضلا عن اتصال أجهزة سطح المكتب والأجهزة المحمولة بالإنترنت. بيد أنه كان من المفترض أن يؤدي مقدمو الخدمة دورا في مكافحة الجريمة السيبرانية بشكل واضح على حد سواء، إلا أن ذلك يتسم بالدقة والتعقيد، حيث يرتبط بأمور مثل التزامات

[1] انظر http://atlas.arbor.net/about/

[2] Higgins, K.J., 2012. Turning Tables: ID'ingThe Hacker Behind The Keyboard. Dark Reading, 2 October, available at : http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240008322/turning-tables-id-ing-thehacker-behind-the-keyboard.html

[3] Simonite, T., 2012.Fighting Hackers without Sinking to Their Level. MIT Technology Review, 26 July, available at : http://www.technologyreview.com/news/428584/fighting-hackers-without-sinking-to-their-level

ومسؤوليات مقدم الخدمة عن محتوى الإنترنت. وفي هذا الصدد، حتى يتسنى دراسة المزيد من احتمالات قيام مزوّد الخدمة بمنع الجريمة السيبرانية، فمن الضروري أولا دراسة عدد من الجوانب الفنية بشكل موجز.

ويقوم مقدمو خدمة الإنترنت بتوصيل المستخدمين بالإنترنت من خلال نقل بيانات بين المستخدمين والأجهزة، مثل الويب والبريد الإلكتروني وخوادم نقل الصوت باستخدام بروتوكول الإنترنت. ويمكن لمزودي خدمة الإنترنت تحليل بعض من حركة البيانات، إلا إذا قام المستخدم بتشفير البيانات من خلال استخدام شبكة افتراضية خاصة، أو خادم وكيل، أو فعالية مُدْمَجة برمجيات للاتصالات. وتشمل بيانات العميل التي يمكن لمزوّد خدمة الإنترنت الوصول إليها محتوى الاتصالات–النصوص والصور غير المشفرّة الموجودة على المواقع الإلكترونية أو في البريد الإلكتروني–البيانات السياقية مثل أي من الخدمات التي يتم زيارتها، ومصدر وُجْهَة البريد الإلكتروني، وأي الأوقات التي تستخدم فيها خدمات مختلفة، وكم من الوقت يقضيه المستخدم على الخدمات المختلفة، حتى ولو تم تشفير الموقع الأساسي. وبشكل عام، يمكن رصد محتوى البيانات فقط في وقت الإرسال، ثم من خلال مراقبة اتصال المستخدم وتخزين البيانات من خلال استخدام أجهزة متخصصة. والجدير بالذكر أن الاستثناء يتمثل في إدارة مقدم خدمة الإنترنت خدمة مثل خادم البريد الإلكتروني الذي يخزن الرسائل لفترة زمنية أطول.

وغالبا ما يستخدم شخص العديد من مزودي خدمة الإنترنت حيث يقومون بالدخول على الإنترنت من مواقع مختلفة. وغالبا ما يختلف مزوّد الخدمة للمستخدم المنزلي عن نظيره من مقدمي الخدمة المتنقلة، إلى جانب ذلك؛ قد يستعمل المستخدمون مزوّدا أخر عندما يتصلون بالإنترنت في العمل، بالإضافة إلى الاتصال من خلال شبكة لاسلكية في أحد المقاهي المحلي من مزوّد خدمة إنترنت آخر. وبالتالي قد تنشر المعلومات حول أنشطة أحد الأشخاص عبر العديد من المقدمين الآخرين.

ويتحكم مزودو استضافة الإنترنت في الأنظمة التي تعمل بها المواقع والخدمات الأخرى. وفيما يتعلق بالعلاقة بين مزوّدي خدمة الإنترنت وعملائهم، تحظى الشركات المستضيفة بموقع متميّز فيما يتعلق بمرور البيانات من وإلى الخدمات المقدمة إلى عملائها. لذلك؛ فإن لديها الإمكانية الفنية لتعطيل أو منع الاستخدام غير القانوني لتلك الخدمات. وعادة ما تضع الشركات المستضيفة قيودا على طبيعة الخدمات التي يمكن استضافتها معها من خلال اتفاقات الخدمة والتي غالبا ما تتناول السلوك المسيء المعروف مثل إرسال كميات كبيرة من البريد الإلكتروني الطفيلي أو بريد إلكتروني مسيء، فضلا عن استضافة محتوى غير قانوني، أو استخدامها لانتهاك حقوق الطبع والنشر.

ويمكن أن يؤدي مزودو خدمة الإنترنت دورا في منع الجريمة السيبرانية عبر مجالين رئيسيين: (1) عبر تخزين بيانات المستخدم التي يمكن الدخول عليها واستخدامها لاحقا بموجب سلطات إنفاذ القانون في تحقيقات الجريمة

السيبرانية، (2) وأيضا عبر "التصفية" الفَعّالة لمحتوى الإنترنت أو المراسلات التي تتم عبر الإنترنت، والتي تهدف في المقام الأول إلى منع الأفعال التي تنطوي على جرائم سيبرانية. ويتناول هذا القسم الجوانب الفنية والتنظيمية لكل من تلك المجالات.

تخزين البيانات – نظرا لحجم مرور البيانات عبر الشبكات، أصبح من المتعذر لمزودي خدمات الإنترنت الاحتفاظ بسجل كامل لجميع حركة المرور على الشبكة. وقد نفذّت بعض البلدان أنظمة مراقبة مطورة للإنترنت، لكن يمكن أن تمثل القيود التكنولوجية لجمع كميات كبيرة من البيانات وتحليلها تحديا. وقد يحصل تسجيل معلومات أقل تفصيلا (مثل عناوين بروتوكول الإنترنت الخاصة بالمستخدمين في أوقات معينة) خلال فترات زمنية طويلة. وبشكل عام، يستطيع مزوّدو خدمة الإنترنت إجراء مراقبة مستهدفة "في الوقت الحقيقي" للبيانات، و (كما نوقش في الفصل الرابع (السلطات المعنية بإنفاذ القانون والتحقيقات))، وتتطلب قواعد "الاعتراض القانوني" من مزودي خدمة الإنترنت في العديد من الدول أن تكون لديهم القدرة على إجراء مراقبة مستهدفة "في الوقت الحقيقي" للاتصالات الخاصة بالفرد أو الأماكن.

حماية البيانات – يخضع تخزين و البيانات معالجتها بمعرفة مزود خدمة الإنترنت إلى قوانين حماية البيانات التي تفرض شروط على حماية واستخدام المعلومات الشخصية.[1] ففي عام 1990، اعتمدت الجمعية العامة للأمم المتحدة المبادئ التوجيهية لتنظيم استخدام ملفات البيانات الشخصية المحوسبة.[2] وتحتوي تلك المبادئ التوجيهية على عشرة مبادئ بما في ذلك النزاهة والدقة ومواصفات الهدف وأن تنطبق على "جميع الملفات المحوسبة العامة والخاصة". وينص مبدأ الأمن على أنه يتعين حماية الملفات ضد *"الأخطار البشرية، مثل الدخول غير المرخص، أو اختلاس البيانات أو التلوث من خلال فيروسات الحاسوب"*. وقد كشفت مراجعة أجريت في عام 2012 لقوانين حماية البيانات أن وجود قوانين شاملة في 89 بلد مع وجود مشاريع قوانين في 10 بلدان أخرى.[3]

[1] اتفقت منظمة التعاون والتنمية في الميدان الاقتصادي ومجلس أوروبا على مجموعة متماثلة من المبادئ الخاصة بمعالجة البيانات الشخصية في بداية الثمانيات (انظر المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي حول حماية الخصوصية وتدفق البيانات الشخصية عبر الحدود، 1980؛ اتفاقية مجلس أوروبا لحماية الأشخاص فيما يتعلق بالمعالجة الذاتية للبيانات الشخصية، ETS رقم 108، 1981.)وقد اعتمدت المنظمات الإقليمية الأخرى منذ ذلك الحين قواعد حماية البيانات، بما في ذلك منتدى التعاون الاقتصادي لآسيا والمحيط الهادئ، الجماعة الاقتصادية لدول غرب أفريقيا، ومنظمة الدول الأمريكية (انظر إطار الخصوصية لمنتدى التعاون الاقتصادي لآسيا والمحيط الهادئ، 2005 القانون التكميلي A/SA.1/01/10 حول حماية البيانات الشخصية داخل الجماعة الاقتصادية لدول غرب أفريقيا، 2010، وقرار الجمعية العامة2661 حول الوصول للمعلومات العامة وحماية البيانات الشخصية، 2004). وقد وضع الاتحاد الأوروبي مجموعة شاملة من قواعد حماية البيانات في حين أن الحق في حماية البيانات يعتبر جزءا من ميثاق الحقوق الأساسية للاتحاد الأوروبي (فضلا عن الحق الأوسع في الخصوصية، بما في ذلك الاتصالات). ويتضمن التوجيه الخاص بحماية البيانات قواعد مفصلة تنطبق على منظمات القطاع العام والخاص بما في ذلك مزودي خدمات الإنترنت (انظر التوجيه 95/46/EC للاتحاد الأوروبي ومجلس 24 أكتوبر 1995 حول حماية الأشخاص فيما يتعلق بمعالجة البيانات الشخصية وحول حرية نقل تلك البيانات. 23/11/1995 , OJ L 281 صفحة 31-50).

[2] الجمعية العامة للأمم المتحدة، قرار 95/45، 14 ديسمبر 1990.

[3] جرينليف، 2012. قوانين خصوصية البيانات العالمية: 89 بلد، ويتسارع هذا الأمر. قوانين الخصوصية &تقرير الأعمال الدولي، إصدار 115، ملحق خاص.

وتشمل بعض أطر حماية البيانات الإقليمية – مثل الإطار القانوني للاتحاد الأوروبي– قواعد محددة حول حماية البيانات في قطاع الاتصالات الإلكترونية.[1] وفي ظل هذا الإطار، لابد أن تتخذ خدمات الاتصالات المتاحة للجميع "*تدابير فنية وتنظيمية مناسبة للسلامة الأمنية ... في حالة الضرورة بالتزامن مع مزوّد شبكة الاتصالات العام فيما يتعلق بأمن الشبكة*". يمكن معالجة مرور البيانات الخاصة بالمستخدمين لأغراض معينة، ويتعين محوها وعدم الكشف عن هويتها عندما لا يكون هناك حاجة لها (أنظر القسم الفرعي التالي حول استبقاء البيانات). ويمكن أن تقوم الدول الأعضاء في الاتحاد الأوروبي بتقييد تلك الحقوق عند الضرورة لحماية بعض الأهداف، بما في ذلك "*الأمن العام، ومنع الجرائم الجنائية والتحقيق فيها والكشف عنها وملاحقتها قضائيا أو الاستخدام غير المرخص لنظام الاتصالات الإلكترونية*.

وأشارت غالبية البلدان المجيبة خلال جمع المعلومات الخاصة بالدراسة، إلى بعض الأحكام الدستورية أو القانونية لحماية خصوصية البيانات الشخصية. وكان الهدف النموذجي المنصوص عليه في قوانين حماية البيانات هو "*ضبط عملية جمع واستخدام المعلومات الشخصية والكشف عنها بطريقة تميّز كلا من حق الفرد في الخصوصية واحتياجات المعلومات الخاصة بالمنظمة*".[2] أما فيما يتعلق بمساهمة مزوّدي خدمة الإنترنت في منع الجريمة السيبرانية، فإنه يمكن أن تخضع قوانين حماية البيانات لعدد من التأثيرات. وفي العموم، لا ينبغي للقيود المفروضة على معالجة البيانات (عند وجود استثناءات قانونية كافية على الأقل) أن تمنع الدخول القانوني لبيانات أحد عملاء مزود خدمة الإنترنت بموجب إنفاذ القانون لأغراض تتعلق بالتحقيق. هذا، وقد تمثل الاستثناء النمطي المبلغ عنه في أنه "*لا يجوز للكيانات غير المعنية بتطبيق القانون (بما في ذلك الشركة) التي تحتفظ بالمعلومات الشخصية أن تسمح بالكشف عن المعلومات لإحدى هيئات إنفاذ القانون دون انتهاك قانون الخصوصية إلا في حالة "الضرورة الملحة" لإنفاذ القانون الجنائي*".[3]

ومع ذلك؛ قد تؤثر التزامات حماية البيانات التي تتطلب محو البيانات الشخصية عندما لا تكون ثمة حاجة لها للأغراض التي جُمعت من أجلها، على تحقيقات الشرطة في الجريمة السيبرانية. وكما لوحظ على سبيل المثال في الفصل الرابع (سلطات إنفاذ القانون والتحقيقات)، أفاد عددٌ من سلطات إنفاذ القانون بالتحديات المتعلقة باستبقاء مزوّد خدمة الإنترنت للبيانات لفترات قصيرة وربما يُعزى هذا في بعض الأحيان إلى تأثير قوانين حماية البيانات. بالإضافة إلى مساهمة قوانين حماية البيانات، كما هو الحال بالنسبة لجميع المنظمات والأفراد التي

---

[1] التوجيه 2002/58/EC للبرلمان الأوروبي ومجلس 12 يوليو 2002 حول معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية. OJ L 201, 31.7.2002. صفحة: 37-47.

[2] استبيان دراسة الجريمة السيبرانية. السؤال رقم 22.

[3] استبيان دراسة الجريمة السيبرانية. السؤال رقم 24.

تقوم بمعالجة البيانات، في منع الجريمة السيبرانية من منظور مزوّد خدمة الإنترنت وذلك من خلال توفير معايير معالجة بيانات تساعد في ضمان أمن وسلامة بيانات المستخدم.

الاحتفاظ بالبيانات – يعني التأثير المشترك لكل من قوانين حماية البيانات والتداعيات المالية لتخزين كميات كبيرة من البيانات بأن مزوّدي خدمة الإنترنت ليسوا ملزمين بفترات غير محددة لاستبقاء البيانات. وبهدف المساعدة في التحقيقات التي تضطلع بإجرائها هيئات إنفاذ القانون، قدّم عددٌ من الدول استثناءات على قوانين حماية البيانات، وذلك بغية إلزام مزوّدي خدمة الإنترنت بتخزين أنماط معيّنة من البيانات الخاصة بأنشطة العميل على الإنترنت لفترات زمنية (مثل عام)، يمكن من خلالها دخول المحققين إلى تلك البيانات بموجب إذن قضائي أو إداري.

فمن الملاحظ أن أكثر القوانين المعمول بها هو توجيه الاتحاد الأوروبي حول الاحتفاظ بالبيانات،[1] حيث تلزم الدول الأعضاء بالاتحاد الأوروبي مزوّدي خدمات الإنترنت بتخزين البيانات التي يشكلونها والتي تعتبر ضرورية لتعقب مصدر الاتصال وتحديده؛ وكذلك تحديد جهة الاتصال ونوعه وتوقيته؛ فضلا عن تحديد جهاز اتصال المستخدمين. ويتعين تخزين البيانات لفترة تتراوح بين ستة أشهر وعامين. وقد شكّك عددٌ من المحاكم الوطنية في الملاءَمَة والتأثير الواقعي على خصوصية تلك المتطلبات.[2]

وقد نظر عدد قليل من الدول الأخرى في قوانين استبقاء البيانات أو قامت بتنفيذها. فعلى سبيل المثال، اقترحت إحدى بلدان أوقيانوسيا نظاما على غرار ما لدى الاتحاد الأوروبي حيث خضع للنظر من قِبَل لجنة برلمانية مشتركة.[3] ولدى بلد آخر في جنوب أسيا تشريعات تمكن الحكومة من تحديد متطلبات الوسطاء لاستبقاء السجلات الإلكترونية إلا أن مثل تلك القواعد تم تحديدها لمقاهي الإنترنت فقط.[4] وفي المقابل ألغت المحكمة العليا في أحد بلدان أمريكا الجنوبية في عام 2009 قانون الاحتفاظ بالبيانات بناء على أسباب التدخل في حقوق الخصوصية للأفراد.[5]

أعرب المقرر الخاص للأمم المتحدة المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية أثناء مواجهة الإرهاب عن قلقه إزاء *"تبني قوانين استبقاء البيانات في العديد من البلدان دون أي ضمانات قانونية حول*

[1]توجيه البرلمان الأوروبي ومجلس أوروبا 2006/24/EC 15 آذار/مارس 2006 حول استبقاء لبيانات المكونة أو المعالجة بالتزامن مع توفير خدمات إلكترونية متاحة للجميع أو شبكات اتصالات عامة وتعديل التوجيه2002/58/EC (OJ L 105/54، 13 أبريل 2006.

[2]براون، أي. 2010. استبقاء بيانات الاتصالات في إنترنت متطور. المجلة الدولية للقانون وتكنولوجيا المعلومات. المعلومات 19 (2): 95-109.

[3]النائب العام، الحكومة الأسترالية، 2012. تجهيز استراليا ضد المخاطر الظاهرة والمتطورة: ورقة مناقشة تصحب نظر اللجنة البرلمانية المشتركة حول المخابرات والأمن لعدد من أفكار الأمن القومي التي تحتوي على مقترحات إصلاح اعتراض الاتصالات، وإصلاح أمن قطاع الاتصالات وإصلاح التشريعات الخاصة بالاستخبارات الاسترالية.

[4]الخصوصية الدولية. 2012. تقرير البلد: الهند، الخصوصية في دول العالم النامي، يمكن زيارته على الموقع التالي:
https://www.privacyinternational.org/reports/india-0

[5] *Halabi, Ernesto c/ P.E.N. - ley 25.873 (Acción de clase, Argentina*

الوصول إلى تلك المعلومات المقررة أو دون اعتبار أن التطورات التكنولوجية تضفي ضبابية على الاختلاف بين المحتوى وبيانات الاتصالات التي تؤخذ بعين الاعتبار، في حين تطالب النصوص الدستورية بضمانات حول الوصول إلى محتوى الاتصالات، وتكون حماية سجلات المعاملات محدودة بصورة أكبر".[1] لذلك فعلى الرغم من أنه من الممكن أن تمثل قوانين استبقاء البيانات نهجا عمليا لضمان إمكانية أن يؤدي مزودو خدمات الإنترنت دورا أكبر في منع الجريمة السيبرانية من خلال التعاون المتطور لإنفاذ القانون، فإنه من المهم تنفيذ تلك القوانين بضمانات إجرائية كافية وحماية للخصوصية.

الإخطار عن اختراق البيانات – وأخيرا، يمكن أن يتأثر تخزين مزوّد خدمة الإنترنت لبيانات العميل بمتطلبات "*التقرير الإجباري بوجود اختراق أمني*". حظي التقرير الإلزامي بوجود اختراق أمني لدى الأطراف المتضررة والمنظمين خاصة عندما يتم الكشف عن تلك البيانات الشخصية، بدعم واسع في العديد من البلدان. ويهدف الإخطار إلى تمكين ضحايا الاختراق من اتخاذ التدابير التي من شأنها أن تقلل واقع التأثير الأمني (مثل تغيير كلمات المرور أو أرقام التعريف الشخصي أو طلب إعادة إصدار بطاقات الدفع)؛ وذلك لزيادة الضغط التنافسي بشأن الأعمال التجارية لتحسين أمنها؛ وكذلك دعم عمل المنظمين المسئولين عن حماية البيانات، فضلا عن حماية البنية التحتية الحيوية.

وتوجد قوانين الإخطار باختراق البيانات على المستوى دون الوطني في بلدان في أمريكا الشمالية.[2] ويلزم الاتحاد الأوروبي شبكات وخدمات الاتصالات العامة بإعداد تقرير حول الاختراقات الهامة للسلطات الوطنية،[3] والتي تؤثر سلبا على الأفراد.[4] وتنظر في الوقت الراهن تمديد هذا المتطلب ليشمل جميع المنظمات الضالعة في معالجة البيانات الشخصية.[5] وقد تم أيضا تقديم متطلبات أو توجيهات الإخطار بمعرفة البلدان الموجودة في أوقيانوسيا وجنوب شرق أسيا وجنوب أسيا.[6]

---

[1] مجلس الأمم المتحدة لحقوق الإنسان، الدورة الثالثة عشرة، A/HRC/13/37، 28 كانون الأول/ ديسمبر 2009، صفحة: 16.

[2] المؤتمر الوطني للمجالس التشريعية في الدولة، 2012. قوانين الدولة الخاصة بالإخطار بوجود اختراق أمني، بالموقع التالي
http://www.ncsl.org/issuesresearch/telecom/security-breach-notification-laws.aspx

[3] المادة 13أ للتوجيه EC/21/2002 للبرلمان الأوروبي ومجلس 7 مارس 2002 حول الإطار التنظيمي المشترك لشبكات وخدمات الاتصالات الإلكترونية (OJ L 108، 2002/4/24، صفحة: 33-50).

[4] المادة 4 من التوجيه 2002/58/EC للبرلمان الأوروبي ومجلس 12 يوليو 2002 الخاص بمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية (OJ L 201، 2002/07/31، صفحة: 37-47).

[5] المادة 31 و 32 للمقترح الخاص بتنظيم البرلمان الأوروبي والمجلس المعني بحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وكذلك حرية نقل مثل تلك البيانات. COM(2012) 11 final

[6] Maurushat, A., 2009 قانون الإخطار باختراق البيانات عبر العالم من كاليفورنيا إلى استراليا. قانون الخصوصية والأعمال الدولية. ورقة بحث قانون UNSW رقم. 11-2009.

وعلى الرغم من أن إخطارات اختراق البيانات تمثل عنصرا هاما لأنظمة أمن المعلومات، بما في ذلك تلك التي تنطبق على مزودي خدمة الإنترنت، فإنه ينبغي للقوانين تعريف ماهية "الاختراق الأمني" بشكل حذر وأن تستخدم بالتزامن مع مجموعة من التدابير، بما في ذلك قوانين حماية البيانات الفعّالة.

تنقية محتوى الإنترنت – بالإضافة إلى فرص منع الجريمة المتعلقة بتخزين البيانات، فإن مزوّدي خدمة الإنترنت يمكن أن يؤدوا دورا دورا في منع الجريمة السيبرانية من خلال المراجعة النشطة لاتصالات الإنترنت وكذلك البيانات التي تحملها. وجدير بالذكر؛ أن أحد المفاهيم الرئيسية في هذا الصدد يتمثل في إمكانية " تَنْقِيَة" الإنترنت بمعرفة مزودي خدمة الإنترنت.

وتحدث تَنْقِيَة اتصالات الإنترنت عند مستوى معين على جميع الشبكات تقريبا. ويستخدم المستوى الأساسي للتصفية لتحسين أداء الشبكة وكذلك الأمن من خلال استبعاد البيانات غير الصحيحة أو التالفة. ومن الممكن أن يكون لدى مزوّدي خدمة الإنترنت القدرة الفنية على تصفية المحتوى الضار أو غير القانوني. وينفذ الكثير من مزوّدي خدمة الإنترنت تصفية أساسية للبريد المزعج لحسابات البريد الإلكتروني لمستخدميهم، كما يمكنهم أيضا، على سبيل المثال، بسط الحماية ضد بيانات المرور الضارة والمعروفة والتي تسببها الفيروسات، أو محاولات القرصنة من خلال رفض حركة مرور البيانات التي يتم التعرف عليها في هذه الحالة.

البريد الطفيلي وشبكات الروبوت – تشكل تصفية البريد الطفيلي مصدر قلق كبير لجميع مزودي خدمات البريد الإلكتروني نظرا للكمية الكبيرة لرسائل البريد المزعج المرسل والوارد كل يوم. وتعتبر الطريقة التي تتم بها تصفية البريد المزعج مختلفة ومعقدّة، بما في ذلك تحليل مصدر البريد الإلكتروني للتعرف على مصادر البريد المزعج وكذلك التحليل النصي للتعرف على الأنماط والعبارات الشائعة للمحتوى في الرسائل. ويتم استبعاد الرسائل التي يتم التعرف عليها باعتبارها بريدا مزعجا بشكل كامل، أو يتم تقديمها للمستخدم باعتبارها "مجلدات البريد المزعج". بالإضافة إلى تصفية البريد المزعج، يمكن أن يؤدي مزودو خدمات الإنترنت دورا في مكافحة بيانات المرور الضارة، مثل تلك المكونة من خلال شبكات حواسيب مصابة.

وعندما يتم إخطار مزودي خدمات الإنترنت، أو التعرف من خلال أنماط بيانات مرور الإنترنت، أن جهازا في شبكتهم يبدوا جزءا من شبكات حواسيب مصابة أو مصابا ببرامج ضارة، فيتمثل أحد الخيارات في منع بعض أو جميع بيانات المرور من ذلك العنوان. في حين يتم إخطار العميل بالخطوات التي يمكنه اتخاذها لإزالة البرامج الضارة. يمكن أن تصدر تلك الإخطارات من شركات الأمن التي تراقب شبكات الحواسيب المصابة من خلال استخدام تقنيات مثل أجهزة "مصيدة قراصنة الإنترنت" التي تجذب على نحو متعمد البرامج الضارة. كما يمكن لمزودي خدمة الإنترنت اتخاذ خطوات للمبادرة في تحديد الأجهزة الخطرة من خلال مراقبة مرور البيانات

لتوقيعات معروفة، على الرغم من الحاجة إلى بعض الاستهداف لجعلها فعّالة. وقد خلصت نشرة صادرة من الشبكة الأوروبية ووكالة أمن المعلومات إلى أن "التعرف على بيانات حركة شبكة الحواسيب المصابة من بين بيانات حركة عادية وغير ضارة هو مثل البحث عن إبرة في 100 مليون كومة قش". وكما لوحظ أعلاه وفي الفصل الخامس (سلطات إنفاذ القانون والتحقيقات)، فإن مراقبة بيانات الحركة العامة يمكن أن تؤدي، في بعض الأحوال، إلى خطورة التعارض مع حماية البيانات وقوانين الخصوصية.[1]

تنقية المحتوى – وكما نوقش أعلاه في إطار مسؤولية مزود خدمة الإنترنت، تلزم القوانين مزودي خدمة الإنترنت في بعض البلدان أن يقوموا بمنع الوصول إلى المحتوى غير القانوني مثل استغلال الأطفال في المواد الإباحية. فثمة أساليب مختلفة يمكن لمزود خدمة الإنترنت أن يقوم بها بجانب أساليب مختلفة تجعل المفاضلة بين السرعة والتكلفة والفاعلية والدقة. ومن خلال تصفية نظام أسماء النطاقات، يمكن لمزودي خدمة الإنترنت التحكم في الإجابات الممنوحة للمستخدمين من خلال خادم نظام أسماء النطاقات، وبالتالي تقييد الوصول إلى نطاق مثل "google.com"، لكن لا يقيد الوصول لصفحة معينة أو مجموعة من نتائج البحث. وهذا أمر يسهل تجاوزه حيث يمكن أن يستفيد المستخدمون من خوادم نظام أسماء النطاقات التبادلية لمنح نتائج حقيقية. ويمكن استخدام رأس برتوكولات الإنترنت لمنع حواسيب الأفراد وفقا لعناوينهم أو منع بعض الخدمات جزئيا مثل الويب أو البريد الإلكتروني. فكما هو حال الكثير من المواقع التي يتم تشغيلها على خادم إنترنت واحد، فإنه من الممكن أن تؤثر على المواقع غير ذات الصلة – ويكون ذلك بأعداد كبيرة في بعض الأحيان. ويمكن استخدام "فحص حزم البيانات" لفحص الجزء الرئيسي من بيانات مرور الإنترنت. الأمر الذي يتيح تصفية مرنة للغاية، إلا أنه يتطلب أجهزة باهظة الثمن على روابط عالية السرعة لمزودي خدمات الإنترنت، كما يمكنها إبطاء جميع وصلات المستخدم.

عمليا، يستخدم العديد من أنظمة التصفية مجموعة من تلك الأساليب لتشكيل مرشح مُهَجّن، وغالبا ما يتم استخدام مرشحات أبسط مثل تلك الموجودة في نظام أسماء النطاقات لتحديد مرور البيانات حتى يتم إعادة توجيهها لمرشحات أكثر تعقيدا. ويتيح أسلوب التهجين تصفية مُتَطَوّرة بموارد منخفضة بشكل كبير.

ومن بين الأمور الأخرى الممكنة التي يتصدى لها مزودو خدمات الإنترنت للمحتوى غير القانوني هو إبطاء مرور البيانات بدلا من حجبها تماما. ويمكن استخدام هذا الأسلوب لجعل الخدمة غير طبيعية بحيث يتجنبها المستخدمون. ومن بين تلك الأمثلة إبطاء وصلات الويب المشفرة، لإجبار المستخدمين على أن تكون غير

[1] Hogben, G., (ed.) 2011. Botnets: Detection, Measurement, Disinfection &Defence. ENISA, pp.73-74

مشفرة، ومن ثم نسخ المواقع القابلة للفحص، وكذلك "تقييد" ممارسة مزوّد خدمة الإنترنت لحركة تبادل الملفات مثل برتوكول مشاركة الملفات عبر الإنترنت.

وقد أثارت إمكانيات تصفية أو منع المحتوى، بما في ذلك تلك التي تهدف إلى منع الجريمة السيبرانية، عددا من شواغل حقوق الإنسان. وعلى سبيل المثال، أكد مجلس حقوق الإنسان على أهمية الوصول إلى الإنترنت باعتباره من حرية التعبير وكذلك حقوق الإنسان الأخرى. ويؤكد القرار الذي اعتمدته في دورتها العشرين على "أن نفس الحقوق التي يتمتع بها الناس عند عدم الاتصال ينبغي حمايتها على الإنترنت، خاصة في حرية التعبير"، و "تدعوا جميع الدول لتعزيز الوصول إلى الإنترنت وتسهيلها".[1] كما وصف المقرر الخاص للأمم المتحدة المعني بتعزيز وحماية حقوق الإنسان الإنترنت بأنه "أداة لا يمكن الاستغناء عنها لتحقيق مجموعة من حقوق الإنسان، من بينها مكافحة عدم المساواة، وتسريع التنمية والتقدم البشري ... لذلك يتعين أن يكون تسهيل الوصول إلى الإنترنت لجميع الأفراد أولوية لجميع الدول، مع وضع قيود قليلة قدر الإمكان على محتوى الإنترنت".[2]

مسؤولية الوساطة – ترتبط تصفية محتوى الإنترنت ارتباطا وثيقا بإمكانية تحميل مزود الخدمة مسؤولية المحتوى. وعادة ما يكون لمزودي خدمة الإنترنت مسؤولية محدودة بوصفهم "مجرد قنوات" للبيانات. ومع ذلك؛ وكما نوقش أدناه، وخاصة في إطار استضافة الإنترنت، يمكن أن يزيد تعديل المحتوى المنقول من المسؤولية في بعض الأنظمة القانونية، وكذلك في حال كونهم على علم، فعليا أو استدلاليا، بنشاط غير قانوني. ومن ناحية أخرى، يمكن أن تحد الإجراءات العاجلةُ من المسؤولية بعد الإخطار.[3]

تشمل العديد من الأنظمة القانونية مفاهيم المسؤولية الثانوية، حيث يكون أحد الأطراف الذي شارك في أعمال غير مشروعة بالنسبة للآخر مسئول بشكل جزئي عن الضرر الناتج. وعندما أصبح الإنترنت يستخدم على نطاقٍ واسعٍ في منتصف 1990 أثيرت المخاوف بشأن تأثير ذلك على الاقتصاد الرقمي الناشئ لعدم اليقين بشأن المسؤولية عن مزودي خدمات الإنترنت والمضيفين للمحتوى عبر الإنترنت. وفي رد على ذلك، سن عدد من البلدان تشريعاتٍ "أفقية" تحدّ من هذه المسؤولية عبر مجالات متعددة من القانون. تحمي هذه الأحكام بوجه عام الوسطاء من المسؤولية عن نقل أو استضافة محتوى الآخرين، طالما أنهم يستوفون شروط معينة، ولاسيما إزالة محتوى معين عندما يوجه إليهم إخطار بذلك. كما قدم عدد من البلدان أيضا تشريعا "رأسيّا" بشأن المسؤولية

[1] A/HRC/20/L.13, 29 June 2012.

[2] A/HRC/17/27, 16 May 2011.

[3] See OECD2011. *The role of Internet intermediaries in advancing public policy objectives*. DSTI/ICCP(2010)11/FINAL, p.46

الثانوية في مجالات معينة، مثل حماية الأطفال والبيانات الشخصية والتزييف والتشهير والغش في الدفع وأسماء النطاق ولعب القمار على الإنترنت.[1]

قدمت بلدان في أمريكا الشمالية وأوروبا اثنين من أقدم الأنظمة الأفقية لها عدد من العناصر المشتركة. فعلى سبيل المثال، يحتوي التشريع في إحدى بلدان أمريكا الشمالية على قيد واسعٍ على مسؤولية مزود الخدمة، باستثناء المتعلقة بخصوصية الاتصالات وقانون الملكية الفكرية والقوانين الجنائية الاتحادية، وينص التشريع على أنه *"لا يعامل أي مقدمٍ أو مستخدمٍ لخدمة الحاسوب التفاعلية معاملة الناشر أو المتحدث لأي معلوماتٍ مقدمة من قبل مقدم محتوى معلوماتٍ آخر... ولا يرفع أي سبب للدعوى ولا تفرض أي مسؤولية بموجب أي قانونٍ دوليٍ أو محليٍ يتعارض مع هذا القسم"* .[2]

يحمي التوجيه الصادر عن الاتحاد الأوروبي بشأن التجارة الإلكترونية[3] على نحو مماثل مقدمي خدمات الإنترنت وغيرهم من "مقدمي الخدمات الوسيطة" الذين يقدمون السلع أو الخدمات عبر الإنترنت، كما أنه يستبعد العديد من المجالات القانونية بما في ذلك الضرائب وحماية البيانات، والاحتكارات والمقامرة. أما بالنسبة لمزود خدمات الإنترنت "كمجرد قناة" إرسال، فيجب على دول الاتحاد الأوروبي "ضمان أن مزود الخدمة ليس مسئولا عن المعلومات المرسلة". كما أن الخدمات التي تخزن المعلومات بشكلٍ مؤقتٍ ليمكن إحالتها بشكلٍ أكثر كفاءة فهي محميةٌ أيضا، شريطة أن تلتزم بالقواعد المتعلقة بالوصول إلى تلك المعلومات وتحديثها، وإزالة أو إعاقة الوصول إلى المعلومات عقب ملاحظة أن أساس المصدر قد أزيل. وعلى مضيفي المحتوى إزالة المعلومات المخالفة بشكلٍ عاجل أو إعاقة الوصول إليها عند الحصول على المعرفة الفعلية أو الاستدلالية بوجودها.

هذا، ولا يحق لدول الاتحاد الأوروبي فرض التزام عامٍ على مقدمي الخدمة لرصد المعلومات التي يقومون بنقلها أو تخزينها، أو *"البحث بنشاطٍ للحصول عن حقائق أو ظروف تشير إلى نشاطٍ غير قانوني"* . ومع ذلك، فإن للمحاكم أو السلطات الإدارية أن تطلب من مقدمي الخدمات *"إنهاء أو منع المخالفة"* أو وضع *"الإجراءات التي تنظم إزالة أو إعاقة الوصول إلى المعلومات"* .[4]

وقد تم إيلاء حقوق الطبع والنشر القدر الأكبر من الاهتمام في نطاق أنظمة المسؤولية المحددة. ففي إحدى بلدان أمريكا الشمالية، فإن المسؤولية الثانوية لانتهاك حقوق الطبع والنشر محددة على وجه التحديد

---

[1] المرجع السابق.

[2] 47 USC § 230 - Protection for private blocking and screening of offensive material

[3] التوجيه 2000/31 المفوضية الأوروبية الصادر عن البرلمان الأوروبي ومجلس أوروبا في تاريخ 8 يونيو 2000 على بعض الجوانب القانونية لخدمات مجتمع المعلومات، لاسيما التجارة الإلكترونية في السوق الداخلية. OJ L 178, 17 July 2000, pp.1–16.

[4] المرجع السابق

بواسطة التشريع.[1] وهذا من شأنه أن يخلق ملاجئ آمنة لمقدمي الخدمة الذي يقدمون اتصالات شبكة رقمية عابرة، وأنظمة تخزين مؤقت واستضافة المحتوى، وأدوات موقع المعلومات. ويتطلب ذلك عموما نظام إشعار وتفكيك، وسياسة لإنهاء حسابات أصحاب المخالفات المتكررة، وتجهيز تدابير تقنية مستندةٍ إلى معايير للتحكم في الوصول إلى الأفعال. هذا، ويجوز لأصحاب الحقوق رفع دعوى قضائية للحصول على أمر قضائي يمنع الوصول إلى المواد المخالفة، وإنهاء حسابات المشتركين، أو غيرها من الإعانة "الفعالة نسبيا" والتي تكون "أقل عبئا" على مزود الخدمة لذلك الغرض.

ولقد انعقدت مناقشة دولية واسعة أيضا تتعلق بمسؤوليات الوسطاء في اتخاذ إجراءٍ إزاء استغلال الأطفال في المواد الإباحية. وطالب عدد من البلدان في جنوب أوروبا وشرق وغرب آسيا وأوقيانوسيا مقدمي خدمات الإنترنت بمنع وصول العملاء إلى المواقع المنوّه احتواؤها على هذه المواد.[2] ويحتفظ الانتربول بقائمة في جميع أنحاء العالم لعناوين المواقع التي تحتوي على مواد ذات "طبيعة عنيفة"، والتي صدرت تعليمات لمزودي خدمة الإنترنت في بعض البلدان بمنعها بموجب قوانين الاتصالات السلكية واللاسلكية. وقد رفض البرلمان الأوروبي، مع ذلك، اقتراحا تشريعيا من المفوضية الأوروبية والذي من شانه أن يفرض حظرا إلزاميا على مقدمي خدمات الإنترنت عبر الاتحاد الأوروبي، تاركا القرار للدول الأعضاء.[3]

إجمالا، يستطيع مقدمو خدمات الإنترنت ومقدمو خدمات الاستضافة أداء دورٍ رئيسيٍ في منع الجريمة السيبرانية بسبب وضعهم الذي يتيح لهم ربط الأفراد والمنظمات بالأنترنت. إن بإمكانهم الاحتفاظ بالسجلات التي يمكن استخدامها للتحقيق في النشاط الإجرامي؛ ومساعدة العملاء في تحديد الحواسيب الخطرة؛ وحظر بعض أنواع المحتويات غير القانونية مثل البريد المزعج؛ ودعم بيئة اتصالات آمنة لعملائهم بشكل عام. وتتطلب قوانين حماية البيانات في كثير من البلدان من مقدمي خدمات الإنترنت حماية بيانات العملاء، وتحتاج من سلطات التحقيق ضمان سياسة وصول إلى هذه البيانات بشكل متناسب. كما يجب وضع قواعد حرية التعبير في الحسبان في التشريع الذي ينص على التدخل في مجرى تدفق المعلومات عبر شبكة الإنترنت. لقد كانت الحماية من المسؤولية بالنسبة لمقدمي خدمات الإنترنت وغيرهم من الوسطاء عاملا أساسيا في النمو السريع للخدمات على شبكة الإنترنت، في حين وضع مسؤوليات معينةٍ على عاتق مقدمي خدمات الإنترنت، مثل الإجراء عند تقديم إشعار التعدي على حقوق النشر والتأليف والمخالفات الأخرى.

[1] 17 USC § 512 - Limitations on liability relating to material online

[2] See OECD2011. *The role of Internet intermediaries in advancing public policy objectives*. DSTI/ICCP(2010)11/FINAL, p.46

[3] المادة 25 (2) من التوجيه 92/ 2011 الصادر عن الإتحاد الأوروبي بشأن مكافح الاعتداء الجنسي والاستغلال الجنسي للأطفال واستغلالهم في المواد الإباحية، واستبدالقرار إطار المجلس2004/68/JHA(OJ L 335 , 17.12.2011)

تعد المؤسسات الأكاديمية والمنظمات الحكومية الدولية من الجهات الفاعلة الهامة في منع الجريمة السيبرانية ومكافحتها. ومن الممكن أن تسهم هذه المؤسسات، على وجه الخصوص، من خلال تطوير ومشاركة المعرفة؛ وتطوير التشريعات والسياسات؛ وتطوير التكنولوجيا والمعايير التقنية؛ وتقديم المساعدة الفنية؛ والتعاون مع سلطات إنفاذ القانون.

تطوير المعرفة ومشاركتها – ردا على المطالب الحكومية والصناعية للمهنيين العاملين في مجال الأمن السيبراني واحتياجات تنمية القوى العاملة، أننشات المؤسسات الأكاديمية برامج تعليمية متخصصة ومناهج دراسيةٍ، ومراكزَ تدريبٍ لترسيخ المعرفة والبحث، وزيادة التآزر في المعرفة عبر المجالات والفروع. ويقدم عدد متزايد من الجامعات درجات وشهادات وتعليم مهني في المجالات المتعلقة بالأمن السيبراني والجريمة السيبرانية بهدف تعزيز "تثقيف وتدريب الشباب المراهقين ومهنيي المستقبل بخصوص ممارسات الحوسبة الآمنة والمسائل التقنية"[1] كما تعزز الجامعات أيضا من التعليم التطبيقي وتطوير الشبكات الاجتماعية ضد الجريمة السيبرانية من خلال تنظيم ورش العمل والمؤتمرات، مما يوفر فرصا لتبادل المعلومات وتقديم المشورة بشأن التدابر الوقائية والاستجابة، وثقافة التعاون غير الرسمي، وأحيانا، آليات الإبلاغ عن فعل معين وتطوير الحلول التقنية.

وتنبع جهود المساهمين الأكاديميين للسيطرة على الجريمة السيبرانية من مجموعة واسعةٍ من التخصصات، بما في ذلك علوم وهندسة الحاسوب، والقانون، وعلم الجريمة وعلم الاجتماع. هذا، وقد شهد العقدان الماضيان نموا كبيرا في عدد من الدوريات الأكاديمية المخصصة للمسائل المتعلقة بالفضاء الإلكتروني والأمن السيبراني والجريمة السيبرانية.[2] وقد أثمر الوعي والبحوث بشأن القضايا ذات الصلة في عدد متزايدٍ من التقارير الفنية والبحوث والمطبوعات ومنشورات استعراض الأقران وتحليل بيانات الوكالة وبحث غير منشور مملوك لأحد الأشخاص.

تطوير التشريعات والسياسة – يقدّم متخصصو الجامعة إسهاما كبيرا في تطوير وتعديل التشريعات والسياسات، حيث يضطلع الأكاديميون بتقديم المشورة القانونية على المستوى الوطني والإقليمي والدولي، بالإضافة إلى إعداد التشريعات بشأن مجموعة من المواضيع، بما في ذلك التجريم والسرية والخصوصية والحماية الدستورية والقانونية. يتم تقديم هذه النصائح من خلال مجموعة من الآليات، بما في ذلك المشاركة في مجموعات استشارية

[1] استبيان بخصوص دراسة بشأن الجرائم السيبرانية منظمة حكومية دولية والأوساط الأكاديمية) السؤال رقم 70.

[2] يشمل على سبيل المثال، علم النفس السيبراني مجلة البحوث النفسية في الفضاء السيبراني؛ الفضاء السيبراني والملكية الفكرية .الأدلة الرقمية والتوقيع الالكتروني القانون الاستعراضي؛ مجلة القانون والحرب السيبرانية .المجلة الدولية للسلوك السيبراني، علم النفس، والتعلم؛ المجلة الدولية للمجتمع السيبراني والتعليم؛ المجلة الدولية للأخلاق السيبرانية في التربية والتعليم.المجلة الدولية للحروب السيبرانية والإرهاب .المجلة الدولية لعلم الجرائم السيبرانية؛ المجلة الدولية للأمن الإلكترونية والطب الشرعي الرقمي .ومجلة القانون التجاري الدولي والتكنولوجيا.

وأفرقة العمل والعقود الفردية والمؤسسية ومن خلال برامج المساعدة الفنية. نوّه أحد المجيبين الأكاديميين، على سبيل المثال، إلى أن مراكز بحوث الانترنت المتخصصة تكون بمثابة منسقة في كثيرٍ من الأحيان: "لأنشطة الباحثين المتخصصين في مجالات العمل المختلفة المتعلقة بالجريمة السيبرانية (علم الجريمة والخبرات القانونية والفنية)."

المعايير التكنولوجية والفنية – تشرع الجامعات في الأبحاث العلمية التطبيقية البحتة في تكنولوجيا الحاسوب، إما في سياق القطاع الأكاديمي الخاص أو التعاون الحكومي، أو الأبحاث التي يشرف عليها داخليا وخارجيا، أو كوسيلةٍ لتأمين شبكة الجامعات. كما تسهم الجامعات أيضا في علوم الحاسوب وتحاليل الأدلة وتحاليل بيانات الوكالة. بالإضافة إلى الأبحاث الواردة المؤسسات والأفراد، تمثل الجامعات أيضا شركاء مهمين ومنسقي تعاون، من خلال المشاركة في المنظمات المهنية ومنظمات المعايير، فضلا عن مجموعات العمل الفنية. هذا، وقد نوّهت صراحة بعض استراتيجيات الأمن السيبراني بدور الجامعات في الجهود المبذولة لتأمين الفضاء الإلكتروني.[1]

المساعد الفنية – غالبا ما تقوم الجامعات بتصميم برامج المساعدة القانونية في مجال الجريمة السيبرانية وتسليمها لهيئات إنفاذ القانون الدولي ووكالات الأمن الوطني والعدالة الجنائية. كما تقدم الجامعات أيضا المساعدة الفنية للشركات ومؤسسات الشركات الصغيرة والمتوسطة والمؤسسات الأكاديمية الأخرى. تتناول هذه البرامج مجموعة من المجالات الفنية المتعلقة بأساليب التحري وحفظ الأدلة والطب الشرعي الرقمي؛ وتحليل محتوى تحليل البرمجيات الخبيثة (تمييزا لها عن التحليل الجنائي)؛ والسياسة والحكم والامتثال؛ وصياغة وتعديل التشريعات ودعم المحاكمات والملاحقات القضائية.[2] قام العديد من الجامعات بالتزامن مع تطوير أنشطة المعرفة والمساعدة الفنية، بتطوير برامج تعليمٍ خاصة، على سبيل المثال، في تحقيقات الجريمة السيبرانية والأدلة الجنائية الرقمية، والتي تساند بشكل رسمي موظفي السلطات الحكومية والشرطة باعتبارهم طلاب علم.

التعاون مع سلطات إنفاذ القانون – قد يكون لدى سلطات إنفاذ القانون حوافز للتعاون مع الجامعات بسبب الجريمة السيبرانية على مستوى الجامعات وخبرة الأمن السيبراني. وتتعاون الجامعات المستجيبة مع هيئات إنفاذ القانون في تطوير المعرفة والمعايير الفنية والمساعدة الفنية، على الرغم من أن العديد من الأكاديميين المجيبين أشاروا أيضا إلى عدم وجود تفاعل مباشر مع هيئات إنفاذ القانون.[3] كما يسلّط الأكاديميون المستجيبون الضوء، في كثير من الأحيان، على أن توفر الموارد لتوسيع هذه الجهود التعليمية والاتصالات يعتبر إحدى الشواغل. كما

[1] من بين البلدان التي تشير استراتيجيها الوطنية تحديدا إلى تحديدا إلى المؤسسات الأكاديمية والجامعات بوصفهم الجهات الفاعلة الأصليين والشركاء في استراتيجيات الأمن السيبراني الوطنية الخاصة بهم أستراليا وجمهورية التشيك واستونيا وألمانيا والهند واليابان، هولندا، نيوزيلندا، نيجيريا، المملكة المتحدة والولايات المتحدة الأمريكية.

[2] ومن بين الموضوعات الأخرى التعاون الدولي والجريمة المنظمة العابرة للحدود الوطنية، والاتصالات العامة والتكنولوجيا، وقضايا الوقاية.

[3] قد يكون هذا بسبب موقع المجيب ومعرفة إدارة خطر الجامعة والأنظمة والعمليات. كانت غالبية المجيبين الأكاديميين أعضاء هيئة التدريس في مقابل تكنولوجيا المعلومات أو إدارة الخطر أو أفراد الأمن.

نوّه أحد المجيبين، على سبيل المثال، إلى أنه: "لا توجد أسباب مؤسسية عامة للتعاون — لا تملك وكالات الدولة أي معايير أو ميزانية للتعاون مع الجامعات. وبهذا فإن كافة الاتصالات والتعاون القائم يتخذ الشكل غير الرسمي" كما تم اعتبار "التمويل وحجم الموظفين وتوافر الشخصيات الأكاديمية المتخصصة"[1] للمساعدة في جهود السلامة العامة شيء ضروري لتحسين النتائج، ولاسيما زيادة التمويل المخصص للبحث في وسائل الطب الشرعي والتحليل والتدريب والموظفين المهرة.[2] وعلى الرغم من الحاجة إلى "المزيد من الموارد والانفتاح في مجال إنفاذ القانون، وإجراء المزيد من الأبحاث التطبيقية في المجال الأكاديمي،"[3] توجد فرصة كبيرة لتوسيع نطاق التعاون مع المؤسسات الحكومية وسلطات إنفاذ القانون.

[1] استبيان بخصوص دراسة بشأن الجرائم السيبرانية (منظمة حكومية دولية والأوساط الأكاديمية) السؤال رقم 70.

[2] استبيان بخصوص دراسة بشأن الجرائم السيبرانية (منظمة حكومية دوليةوالأوساط الأكاديمية) السؤال رقم 70.

[3] استبيان بخصوص دراسة بشأن الجرائم السيبرانية منظمة حكومية دولية والأوساط الأكاديمية) السؤال رقم 70.

الملحق الأول: شرح الأفعال

أفعال ضد سرية، نزاهة، وتوافر بيانات ونظم حاسوبية	
النفاذ غير المشروع إلى نظام حاسوبي	تشير إلى الأفعال التي تنطوي على الدخول إلى أحد أجزاء النظام الحاسوبي أو الدخول إلى النظام بأكمله، وذلك بدون تصريح أو مبرر لهذا الدخول. وفي هذا الحالة –على سبيل المثال– يقوم أحد الجناة بالتحايل على برنامج الحماية الخاص بالنظام الحاسوبي لأحد المصارف (على سبيل المثال). من الممكن أيضا أن تتمثل هذه الحالة، عند مواصلة أحد المستخدمين البقاء متصلا مع أحد الأنظمة الحاسوبية بعد انتهاء فترة الأذن الممنوح له/لها، مثل؛ قيام أحد الجناة بحجز سعة الخادم لفترة زمنية محددة، ولكن يستمر في الاستعمال بعد انتهاء الفترة الزمنية المسموح بها. هذا، وتتطلب بعض النُهُج الوطنية أن يكون تحايل الجاني مُنصبّا على تدابير الحماية أو تقترن الأفعال بنية مُعَيّنة.
النفاذ غير المشروع إلى بيانات حاسوبية أو اعتراض هذه البيانات أو الاطِّلاع عليها	تشير إلى الأفعال التي تنطوي على الوصول إلى البيانات الحاسوبية بدون تصريح أو مبرر لذلك؛ ويتضمن ذلك الحصول على بيانات أثناء إحدى عمليات الإرسال التي لا يقصد بها أن تكون عَلَانية، فضلا عن الاطلاع على البيانات الحاسوبية (مثل نسخ البيانات) بدون تصريح. وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بالوصول بشكل غير قانوني إلى إحدى قواعد البيانات الحاسوبية، تسجيل عمليات الإرسال بدون حق داخل إحدى شبكات الاتصال اللاسلكي، أو يقوم أحد الجناة، والذي يعمل لدى إحدى الشركات المعنية، بنسخ الملفات وأخَذها بدون تصريح. وتتطلب بعض النُهُج الوطنية أن تكون البيانات ذات الصلة محمية ضد الدخول غير المصرح به. أيضا، تتضمن بعض النُهُج الوطنية اعتراض الانبعاثات الكهرومغناطيسية التي لا يجوز تصنيفها كبيانات حاسوبية. وغالبا ما قد تنطوي أغراض التَجَسّس الصناعي أو التجاري على فعل النفاذ غير المشروع أو اعتراض البيانات الحاسوبية أو حِيَازَة البيانات الحاسوبية.
التدخل غير المشروع في البيانات أو النظم	تشير إلى الأفعال التي تعيق أدَاء أحد الأنظمة الحاسوبية، فضلا عن الأفعال التي تنطوي على ضرر يلحق بالبيانات الحاسوبية أو حذفها أو تَلَفها أو تغيرها أو طَمْسها، وذلك بدون تصريح أو مبرر. وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بإحالة عدد كبير من الطلبات إلى أحد أنظمة الحاسوب والذي من شأنه أن يتسبب في عدم قدرة النظام الحاسوبي على الاستجابة للطلبات المشروعة (وهذا ما يعرف بـ "هجمات الحرمان من الخدمة")، أو حذف ملفات برامج الحاسوب اللازمة لعملية تشْتغِيل أحد خوادم الإنترنت، أو تغيير أحد السجلات في قاعدة

	بيانات أحد الحواسيب. وتغطي بعض النُهُج الوطنية فقط الأفعال ذات الصلة بالبيانات، بيد أن النُهُج الأخرى تتناول أيضا التلاعب في أجهزة الحاسوب. وقد تسبب "القرصنة" في أنظمة الحاسوب المرتبطة بالبنية التحتية للمنشآت الحيوية (مثل شبكات المياه أو إمدادات الكهرباء) في التدخل غير المشروع في البيانات أو إتلاف النظام.
إنتاج أو توزيع أو حيازة أدوات لإساءة استعمال الحواسيب.	تشير إلى الأفعال التي تنطوي على تطوير أو توزيع أجهزة أو برمجيات والتي يمكن استخدامها في ارتكاب الجرائم ذات الصلة بالحاسوب أو الإنترنت. وتتجسد هذه الحالة، على سبيل المثال، عندما يقوم أحد الجناة بتطوير أحد أدوات البرمجيات لتشغيل هجمات الحرمان من الخدمة بشكل آلي. ومن أجل تجنب التدخل في الاستخدام المشروع لهذه الأدوات (مثل من قِبَل خبراء الأمن)، وتتطلب بعض النُهُج الوطنية أن تكون الأداة صُممت خصيصا لأغراض غير قانونية، أو تقترن أفعال أحد الجناة بهدف استعمال الأداة لارتكاب أحد الجرائم.
انتهاك تدابير حماية الخصوصية أو البيانات	تشير إلى الأعمال التي تنطوي على استخدام أحد النظم الحاسوبية لمعالجة المعلومات الشخصية أو نشرها أو الوصول إليها مما يشكل انتهاكا لأحكام حماية البيانات. وتتمثل هذه الحالة، على سبيل المثال، إذا كان أحد الجناة يعمل في أعمال التجارة الإلكترونية وقام بالكشف عن المعلومات الشخصية من قاعدة بيانات عملية التي يتعين عليه الإبقاء على سريتها.
استعمال الحاسوب في أعمال الاحتيال أو التزوير	تشير إلى الأفعال التي تنطوي على التدخل أو النفاذ غير المشروع لأحد الأنظمة أو البيانات الحاسوبية بهدف الحصول على المال بشكل فيه خداع أو تدليس، أو بهدف تحقيق منافع مالية أخرى، أو للتَهَرُّب من دفع إحدى الدُيُون، فضلا عن الأفعال التي تنطوي على التدخل في نظام حاسوبي أو بيانات حاسوبية بشكل ينجم عنه توليد بيانات حاسوبية زائفة. وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بتعديل البرمجيات المستخدمة من قِبَل أحد المصارف لإعادة توجيه تحويل مبلغ مالي إلى حسابه الشخصي، أو إذا قام أحد الجناة بتعديل إحدى رسائل البريد الإلكتروني الصَحِيحة الواردة من إحدى المؤسسات المالية بهدف الاحتيال بشكل أساسي. ويشير أيضا إرسال العديد من هذه الرسائل في مسعى من الجاني للحصول على معلومات شخصية أو للاحتيال إلى "التصيد الاحتيالي". أما فيما يتعلق باستخدام الحاسوب في التزوير، فإن بعض الاتجاهات الوطنية تتطلب أن تكون البيانات الحاسوبية الأصلية تتعلق بوثائق بهدف إنشاء ارْتِباطات قانونية ملزمة. بيد أن الاتجاهات الأخرى تتطلب أن يكون هدف أحد الجناة اعتبار النسخة المعدلة بمثابة التزامات قانونية أو أن تكون لها حجية التزامات قانونية.

جرائم الهوية المرتكبة بواسطة الحواسيب	تشير إلى الأعمال التي تنطوي على إرسال أو حيازة أو استعمال تَعْرِيف شخص آخر مخزن في البيانات الحاسوبية، بدون حق، وذلك بهدف ارتكاب أي نشاط إجرامي غير مشروع أو المساعدة في ارتكابه أو التحريض على ارتكابه. وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة، بدون حق، بالحصول على معلومات رخصة قيادة من أحد الأنظمة الحاسوبية وقام إما ببيع هذه البيانات أو استخدامها لإخفاء هويته الحقيقية عند ارتكابه إحدى الجرائم. وتتطلب بعض الاتجاهات الوطنية أن يقتصر تطبيق هذه الأحكام على أدَوات التعريف المحددة.
جرائم حقوق المؤلف والعلامات التجارية المرتكبة بواسطة الحواسيب	تشير إلى الأفعال التي تنطوي على نسخ المواد المخزنة في البيانات الحاسوبية أو بيانات حاسوبية مولّدة مما يشكل انتهاكا للحماية المفروضة لحقوق التأليف والنشر أو العلامات التجارية. وتتجسد هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بتوزيع أحد الأغاني المحمية بموجب بحق التأليف، وذلك من خلال نظام تبادل الملفات دون ترخيص من الْمُؤَلِّف صاحب المصنف.
إرسال أو التحكم بإرسال الرسائل الطفيلية	تشير إلى الأفعال التي تنطوي على استعمال أحد النظم الحاسوبية في إرسال رسائل إلى عدد كبير من المتلقين بدون تصريح أو طلب. ومن أجل تجنب التدخل في الأعمال الاعتيادية لمراسلات العميل، تتطلب بعض النُهُج الوطنية أن يكون أحد الجناة قام بعنونة هذه الرسالة بمعلومات كاذبة.
الأعمال المرتكبة بواسطة الحواسيب والتي تتسبّب في ضرر شخصي	تشير إلى الأفعال التي تنطوي على استخدام أحد نظم الحاسوب في إزعاج أحد الأفراد، أو التحرش به، أو تهديده، أو تعقبه أو التسبب في خوفه أو ترويعه. وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بإرسال رسائل مُهِينة أو تهديدية أو قَبِيحة، أو صور (أيضا يُشار إلى "التصيد")، أو استعمال أحد نظم الحاسوب في تتبع أو تعقب، أو خلافا لذلك التدخل المادي أو المعنوي في مَصْلَحَة أي فرد. وتستبعد أيضا من هذه الفئة الأفعال التي تشكل قذفا فقط.
الأفعال المرتكبة بواسطة الحاسوب وتنطوي على عنصرية أو كراهية الأجانب	تشير إلى الأفعال التي تنطوي على استعمال أحد نظم الحاسوب في توزيع مواد عنصرية أو تحرض على كراهية الأجانب أو إتاحة هذه المواد، أو استعمال أحد نظم الحاسوب في تهديد أو إهانة أحد الأفراد أو مجموعة من الأشخاص لأسباب عنصرية أو تحمل كراهية للأجانب. وتعني المواد العنصرية أو مواد كراهية الأجانب أي مواد مكتوبة أو صور أو أفكار أو نظريات تدعو أو تشجع أو تحض على التَمْيِيز أو الكراهية أو العنف ضد أي فرد أو مجموعة أشخاص على أساس العرق أو اللون أو النسب أو الأصل القومي أو العرقي، وكذلك الدين إذا ما استخدم كذريعة لتأجيج أي من هذه العوامل.

إنتاج أو توزيع أو حيازة المواد الإباحية المتعلقة بالأطفال بواسطة الحواسيب	تشير إلى الأفعال التي تنطوي على استخدام أحد نظم الحاسوب في انتاج أو إنشاء أو توزيع أو الوصول أو رؤية أو تلقي أو تخزين أو حيازة أي مواد تمثيلية، بأي وسيلة كانت، لشخص حقيقي أو من وحي الخيال يقل عمره عن 18 سنة، أو يبدو أنه أقل من 18 سنة، مارس نشاطا جنسيّا صريحا سواء حقيقيّا أو بالمحاكاة أو أي تصوير الأعضاء الجنسية لطفل لإشباع الرغبة الجنسية بشكل أساسي. وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بتحميل صورة رقمية تبين الاعتداء الجنسي على أحد الأطفال.
الأفعال ذات الصلة بالحاسوب بغرض إغواء أو استمالة الأطفال لأغراض جنسية	تشير إلى الأعمال التي تنطوي على استعمال أحد نظم الحاسوب للعرض على أحد الأطفال الذين لم يبلغوا سن الموافقة على اللقاء الجنسي، لغرض ارتكاب إحدى الجرائم الجنسية ذات الصلة. وتتمثل هذه الحالة، على سبيل المثال، إذا قام أحد الجناة بالمحادثة النصية عبر الإنترنت مع أحد الأطفال مدعيا أنه طفل أيضا، ويعرض على الطفل اللقاء، وذلك مع توافر نية الاعتداء على الطفل. ويمكن أن يطُلق على هذا الفعل أيضا "الاستمالة". وتقصر بعض الاتجاهات الوطنية الجريمة على الإغواء الذي يتبعه أي فعل مادي يؤدي إلى لقاء.
أعمال دعم الجرائم الإرهابية بواسطة الحواسيب	تشير إلى الأفعال التي تنطوي على استخدام نظام حاسوبي في دعم جرائم الإرهاب. ويشتمل ذلك على استعمال أحد الأنظمة الحاسوبية في إرسال إحدى الرسائل إلى الجمهور بقصد التحريض على ارتكاب إحدى الجرائم الإرهابية، سواء كان بشكل مباشر أو غير مباشر، حيث يمثل إتيان هذا السلوك خطورة ارتكاب جريمة أو أكثر من الجرائم الإرهابية (استخدام الحاسوب في التحريض على الإرهاب). وهذا يتضمن أيضا استخدام نظام حاسوبي في تقديم الدعم المالي أو جمعه بهدف استعماله –مع وجود الإدراك باستعماله، سواء بشكل كلي أو جزئي– في ارتكاب عمل إرهابي أو إحدى الجرائم الإرهابية (استخدام الحاسوب في الدعم المالي للعمليات الإرهابية). أيضا يتضمن استخدام أحد أنظمة الحاسوب في التخطيط أو الإعداد أو التنظيم لارتكاب عمل إرهابي أو إحدى الجرائم الإرهابية (استعمال الحاسوب في التخطيط لارتكاب جرائم إرهابية). ويقصد بالجريمة الإرهابية أي فعل مجرم طبقا للصكوك القانونية العالمية المعنية بمكافحة الإرهاب، أو يراد به التسبب في وفاة أحد المدنيين أو إلحاق إصابة جسدية جسيمة به، أو أي شخص آخر لا يشارك بدور نشط في الأعمال العدائية من حالة النزاع المسلح. وتعتبر أيضا جريمة إرهابية، متى كان الغرض من الفعل –في سياق طبيعته– ترويع السكان أو إجبار إحدى الحكومات أو إحدى المنظمات الدولية لأداء عمل أو الامتناع عن أداء عمل.

الملحق الثاني: قياس الجريمة السيبرانية

إحصاءات الجريمة المسجلة لدى أجهزة الشرطة

عادة ما تعتبر إحصاءات الجريمة المسجلة لدى أجهزة الشرطة بمثابة الإحصاءات الإدارية الأقرب إلى إحداث الجريمة الفعلية.[1] بالرغم من ذلك؛ فإنه من المعروف أن إحصاءات الجريمة المسجلة لدى أجهزة الشرطة تقوم فقط على الأحداث التي تصل إلى انتباه الشرطة. وبالتالي؛ فإن هذه الإحصاءات عادة (في أغلب الأحيان بشكل كبير) ما تخفي "رقم مستتر" للجريمة.[2]

أما فيما يتعلق بأحداث الجريمة السيبرانية، فإن درجة الاختلاف بين الإيذاء والجريمة المسجلة لدى الشرطة تكون أضعافا مضاعفة. فقد يكون ما أفاد به ضحايا الاحتيال على بطاقات الائتمان في الدراسات الاستقصائية السكانية وحده أكثر من 80 أضعاف مجموع حالات استعمال الحاسوب في الاحتيال والتزوير المسجلة لدى الشرطة في نفس الدولة.[3] وأيضا، طبقا لإحدى الدراسات الاستقصائية السكانية فإن نسبة 21 في المائة فقط من عدد 20,000 من مستخدمي الإنترنت تقريبا في 24 دولة، قد أفادوا بأنهم كانوا ضحايا أفعال الجريمة السيبرانية، كما أشاروا إلى أنهم قد أبلغوا الشرطة عن هذا الفعل.[4]

وقد تواجه إحصاءات الجريمة المسجلة لدى الشرطة صعوبة أخرى تتمثل في وضع نهج وطني مطابق لتحديد ماهية الأنظمة الحاسوبية أو البيانات الحاسوبية التي تنطوي على أحد الأفعال المحددة التي تشكل الجريمة السيبرانية. بيد أن لدى الشرطة الوطنية نظم إبلاغ قائمة على التباين في طرائق تسجيل أحد الأفعال باعتباره جريمة سيبرانية. ويجوز استخدام ملفات التسجيل كمؤشرات، مثل "ما إذا كان الحاسوب هو محل الجريمة" أو "إذا كان الجاني استعمل أحد أدوات الحاسوب لاقتراف الجريمة".[5] هذا، وتقوم ببساطة الاتجاهات الأخرى على المواد الواردة في التشريع الجنائي الوطني، ومن ثم، تتناول فقط عددا محدودا من أفعال الجريمة السيبرانية، مثل "إساءة استخدام الحاسوب".[6] ويتراوح نِطَاق هذه النتائج في إحصاءات الشرطة من نسبة الأفعال "التقليدية" التي يعتبر

---

[1] الأمم المتحدة. 2003. دليل تطوير نظم إحصاءات العدالة الجنائية.

[2] الأمم المتحدة. مؤتمر الأمم المتحدة الثاني عشر للعدالة الجنائية ومنع الجريمة. 2010. حالة الجريمة والعدالة الجنائية في جميع أنحاء العالم: تقرير الأمين العام للأمم المتحدة، A/CONF.213/3 الأول من شباط/فبراير 2010.

[3] UNODC calculation from Study cybercrime questionnaire. Q30; and Symantec. 2012. *Norton Cybercrime Report 2012*.

[4] Symantec. 2011. *Norton Cybercrime Report 2011*

[5] وزارة العدل الأمريكية. مكتب التحقيقات الفيدرالي 2000. نظم الإبلاغ عن الحوادث الوطنية. مُجلّد1: مبادئ توجيهية لجمع البيانات. متاح على الرابط التالي: http://www.fbi.gov/about-us/cjis/ucr/ucr

[6] انظر على سبيل المثال، لجنة الأمم المتحدة الاقتصادية الخاصة بأوروبا، مؤتمر الإحصائيين الأوروبيين. المبادئ وإطار التصنيف الدولي الجرائم للأغراض الإحصائية ECE/CES/BUR/2011/NOV/8/Add.1. 11 تشرين الأول/أكتوبر 2011. الملحق الأول يوجز نظم تصنيف الجرائم الوطنية.

فيها الحاسوب أداة الجريمة أو محل الجريمة إلى الإحصاءات المعنية فقط بالجرائم التقنية المعينة.[1] ففي الحالة السابقة؛ ربما يكون من الصعب فهم ماهية الحد الأدنى لاستخدام أداة الحاسوب "لارتكاب" إحدى الجرائم المعنية.[2] في الحالة اللاحقة؛ يمكن إجراء مقارنات عبر الحدود الوطنية فقط إذا كان التشريع الوطني يعتبر مُكَافِئا للتشريعات الأخرى، بالإضافة إلى استخدام الفئات المماثلة للأغراض الإحصائية ولكي نفهم ما إذا كانت إحصاءات الشرطة – على سبيل المثال – المعنية "باستخدام أحد أجهزة الحاسوب بدون تصريح" في إحدى الدول يمكن مقارنتها مع الإحصاءات المعنية "بالنفاذ غير المشروع إلى إحدى الحواسيب" في دولة أخرى، فإنه من الضرورة تناول أركان الجريمة الأساسية من منظور القوانين الجنائية. وبالتالي، فإن الدفاع عن مقارنات إحصاءات الشرطة بشأن "الجريمة السيبرانية" من الناحية المنهجية يشكل صعوبة بالغة.

وقد تضمنت المعلومات التي تم جمعها لهذه الدراسة طلبا للدول لتقديم عدد الجرائم المسجلة لدى الشرطة طبقا لكل فعل من الأفعال الـ 14 المدرجة في المرفق الأول (شرح أفعال الجريمة السيبرانية). أما فيما يتعلق بوصف كل فعل بإسهاب؛ فقد طُلب من الدول تقديم الإحصاءات المتاحة لديها للأعوام 2008، 2009، 2010، وتحديد ما إذا كانت البيانات المقدمة توافقت مع إحدى الجرائم الخاصة بالفضاء السيبراني أو الجرائم العامة في القانون.[3] على سبيل المثال؛ ما إذا كانت جرائم "النفاذ غير المشروع لنظام الحاسوب" المسجلة لدى الشرطة قد سُجلت تأسيسا على حكم جنائي خاص يتناول هذا الفعل. ومن ناحية الأخرى قد يتوافق تسجيل الشرطة لجرائم استخدام الحاسوب في أعمال الاحتيال والتزوير مع أحد الأحكام الفرعية لجريمة الاحتيال العام، والتي قد حُدّد استعمال حاسوب في ارتكابها.

فمن الملاحظ أن نسبة تقل عن 40 في المائة من الدول التي أجابت على الأسئلة المعنية بإحصاءات الشرطة، عبر الـ 14 فعلا من أفعال الجريمة السيبرانية (والثلاث فئات الإجمالية)، أشارت إلى أن إحصاءات الجرائم المسجلة مُتَوَفّرة. بيد أن نسبة الانتهاء من مجالات البيانات الممكنة بلغت نسبة تقل عن 20 في المائة، عبر جميع أفعال الجريمة السيبرانية والسنوات المشار إليها أعلاه.[4] وقد يشير ذلك إلى التحدي الذي تواجهه الدول في جمع البيانات الإحصائية المسجلة لدى الشرطة بشأن الأفعال السيبرانية. وعندما سألنا عن الأسباب التي تحول دون توافر الإحصاءات، أشار عدد من الدول إلى تحديات التجميع والتقسيم، ويتجسد ذلك في عدم اعتبار الأفعال المطلوبة متميّزة من الأحداث المسجلة، أو أن البيانات الموجودة لا يمكن تدوينها بسهولة طبقا للفئات المستخدمة في الاستبيان.[5] وهذا يبرهن على الصعوبات التي تعتري تحديد أحد الفئات العامة للجرائم السيبرانية والتي استخدمتها

[1] المركز الكندي لإحصاءات العدالة 2002. الجرائم السيبرانية: عملية جمع القضايا والبيانات والموارد لإحصاءات البلاغات الواردة للشرطة.

[2] فعلى سبيل المثال، قد تتضمن الإحصاءات التاريخية عدد من الأحداث المتعلقة "بسرقة السيارات" أو "السطو المسلح/الكسر والدخول" والتي يعتبر الحاسوب إما أداة الجريمة أو محل الجريمة. المرجع السابق.

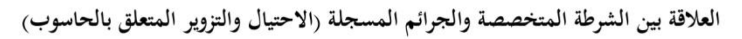
[3] الاستبيان الخاص بالدراسة، السؤال رقم 54–71

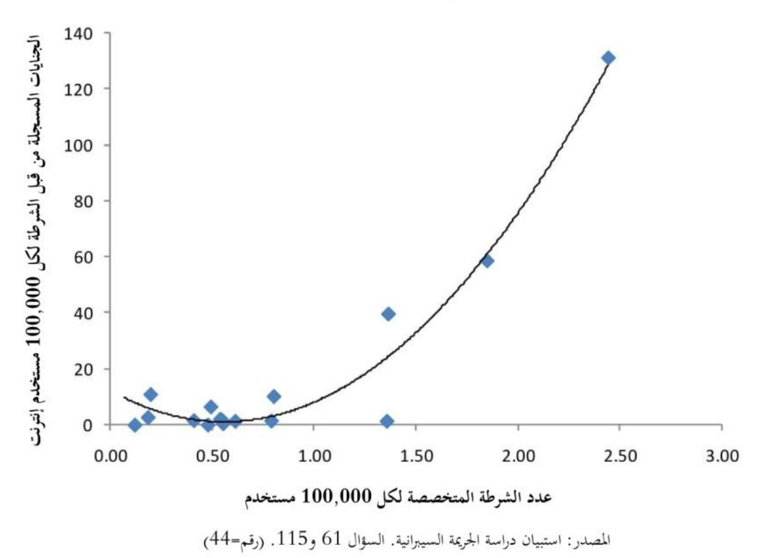
[4] المرجع السابق.

[5] الاستبيان الخاص بالدراسة، السؤال رقم 75

لأغراض إحصائية. وفي هذا الصدد أيضا، ربطت العديد من الدول التحديات في الإحصاءات الشرطية بالأطر القانونية، مع ملاحظة أن عدم وجود حكم قانوني محدد معني بعدم توافق الفئة الإحصائية الشرطية الموجودة. هذا، وقدمت بعض الدول إحصاءات تقديرية في الحالات التي لا يوجد فيها حكم محدد. وفي هذا الشأن، قدمت إحدى الدول، على سبيل المثال، العدد الإجمالي لجرائم الاحتيال والتزوير المسجلة لدى الشرطة، مع تقدير بالنسبة المئوية للجرائم التي ارتكبت باستخدام أحد نظم الحاسوب.[1]

وذكرت إحدى الدول، على سبيل المثال، أن "محدودية الموارد والطبيعة المعقدة "للجريمة السيبرانية" تجعل من الصعوبة البالغة جمع وتحليل المعلومات الإحصائية بغية تقديم صورة كاملة ودقيقة للمشكلة للحكومات والقطاع الخاص ومستخدمي التكنولوجيا." "فغالبا ما تتصادف أركان الجريمة السيبرانية مع الجرائم الجنائية الأخرى، فالعديد من الحوادث لن يلاحظها الضحايا، أو إذا لاحظوها، ففي الغالب لا يقومون بالإبلاغ عنها مطلقا (أو، إذا قاموا بالإبلاغ، فإن من يتقدم بالإبلاغ هم فقط مقدمو الخدمة أو شركات بطاقات الائتمان، والسلطات غير العامة)". بيد أن هناك مشكلة إضافية في هذا المجال تتمثل في حقيقية مفادها أن العديد من الجرائم تعتبر جرائم عبر الحدود الوطنية أو غير معلومة المنشأ، بالإضافة إلى أن العديد من الجرائم تنطوي على ضحايا مستهدفين بشكل جَمَاعِيّ، والتي من شأنها أن تعطي صورا إحصائية مختلفة بناء على ما تم إحصاؤه: ففعل إرسال بريد إلكتروني احْتِيَالِيّ إلى ملايين العناوين يمكن أن يُحسب بمحاولة واحدة أو عدة ملايين من المحاولات، على سبيل المثال، وربما يولد آلافا من الجرائم الكاملة في حالة نجاح المخطط الإجرامي.[2]





المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 61 و115. (رقم=44)

وتظهر عملية فحص إحصاءات الشرطة المقدمة عددا من الأنماط، أولها: توجد دلائل قوية – كما قدمت بيانات الدراسة الإحصائية السكانية القائمة على المجني عليه – على أن تسجل الشرطة للجريمة السيبرانية لا يعتبر مؤشرا جيدا للمستويات الرئيسية للجريمة السيبرانية. فمعدل الجريمة السيبرانية المحددة المسجلة لدى الشرطة قد ترتبط بكل من مستوى النمو في إحدى الدول ووجود شرطة متخصصة.

---

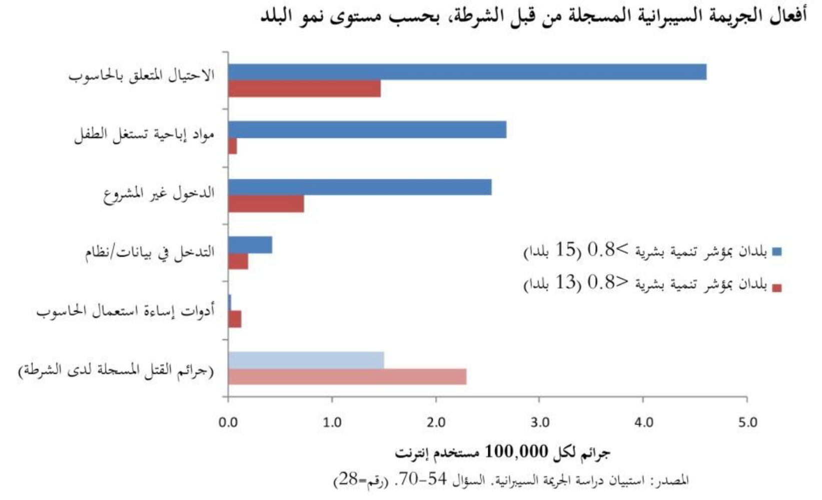
[1] الاستبيان الخاص بالدراسة، السؤال رقم 61

[2] الاستبيان الخاص بالدراسة، السؤال رقم 76.

ويعتبر عدد الدول التي قدمت بيانات صغيرا نسبيا. ومع ذلك؛ تسجل هذه المجموعة المحدودة من الدول، مع تلك الأعداد الكبيرة من الشرطة المتخصصة في الجريمة السيبرانية نسبة عالية من الجريمة السيبرانية، على الأقل فيما يتعلق باستخدام الحاسوب في أعمال الاحتيال والتزوير.[1] وقد أظهرت المقارنة استعمال عدد من الشرطة المتخصصة وعدد من الجرائم المسجلة لكل 100,000 مستخدم من مستخدمي الإنترنت في كل دولة على حدة، بغية تقديم ممخرج عادل للمقارنة.[2]

وربما يعتبر هذا النمط مُفَسّرا بموجب حقيقة مفادها أن إحدى النسب الصغيرة فقط من أفعال الجريمة السيبرانية تصل إلى علم الشرطة في المقام الأول، ويمكن أن تزيد هذه النسبة على الأرجح مع استعمال موارد وقدرات تحقيقية إضافية.[3]

أما النمط الثاني؛ يتعلق بإحصاءات الشرطة ونمو الدولة. فهنالك أربعة أنواع من أفعال الجريمة السيبرانية المسجلة لدى الشرطة–استعمال الحاسوب في أعمال الاحتيال والنصب، جرائم استغلال الطفل في المواد الإباحية، النفاذ غير المشروع لأحد نظم الحاسوب والتدخل في البيانات أو النظام بشكل غير مشروع – ترتفع باستمرار لكل 100,000 مستخدم من مستخدمي الإنترنت في إحدى مجموعات الدول، ويرافق ذلك ارتفاعا في مستويات التنمية البشرية أكثر من مجموعة الدول ذات التطور البشري المنخفض. ويظهر الشكل التالي متوسط عدد الجرائم المسجلة لدى الشرطة لكل 100,000 مستخدم إنترنت في 15 دولة من الدول التي سجلت درجة أعلى من 0.8 بحسب مؤشر التنمية البشرية، بالمقارنة مع 13 من الدول التي سجلت درجة أقل من 0.8 بحسب في مؤشر التنمية

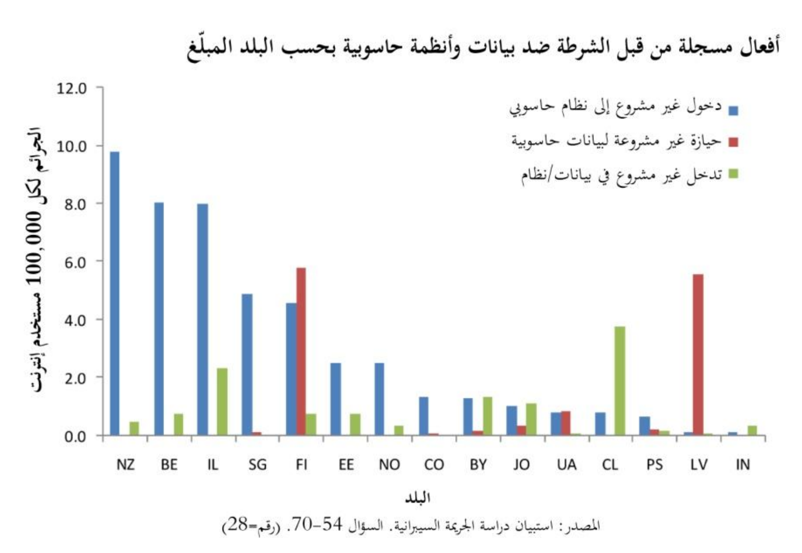


[1] الاستبيان الخاص بالدراسة، السؤال رقم 115، ورقم 61

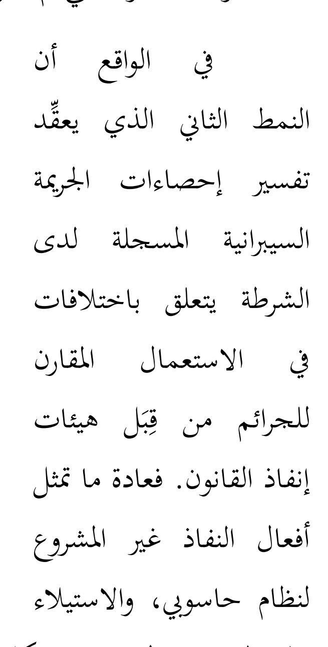
[2] يعتبر مصدر عدد مستخدمي الإنترنت من المؤشرات العالمية للاتصالات السلكة واللاسلكية/تكنولوجيا المعلومات والاتصالات 2012. ويستعمل عدد مستخدمي الإنترنت كقاعدة، بدلا من مجموع السكان، حيث يعتبر الأشخاص الغير متصلين بالإنترنت غير معرضين للإيذاء من الأغلبية الساحقة لأفعال الجريمة السيبرانية، بيد أنه بالرغم من ذلك، توجد أمثلة للحُصُولٌ عَلَى بيانات حاسوبية من أحد الحواسيب المسْتَقِلّة.

[3] See, for example, Harrendorf, S., Smit, P. 2010. Attributes of criminal justice systems – resources, performance and punitivity. *In*: European Institute for Crime Prevention and Control Affiliated with the United Nations (HEUNI). *International Statistics on Crime and Justice*. Helsinki

البشرية.[1] بيد أنه من الجائز أن المستويات المطلقة لبعض هذه الجرائم على الأقل تعتبر في الحقيقة أعلى في الدول الأكثر تقدما. وفي هذا الصدد؛ على سبيل المثال، تدعم نتائج الدراسة الاستقصائية السكانية لاستعمال الحاسوب في الاحتيال على المستهلكين مستوى إيذاء أعلى بقليل في الدول المتقدمة الأكثر تطورا.[2] وبالرغم من ذلك؛ تطرح الدراسة الاستقصائية صورة عكسية لأفعال الجريمة السيبرانية الأخرى المرتكبة من قبل الأفراد، مع وجود مستويات عالية من الإيذاء عادة في الدول الأقل نموا.[3] هذا، وتعتبر صورة موارد الشرطة، مَدْمُوجة بحقيقة مفادها أن مُقَارَنة جرائم القتل[4] المسجلة لدى الشرطة أكبر في مجموعة الدول الأقل نموا، قد تظهر أن قدرات الشرطة في التحقيق في الجريمة السيبرانية في الدول المتقدمة تعتبر مسؤولة بشكل جزئي عن تسيير اختلافات كبيرة بين مجموعتين الدول التي تم تناولهما.



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 54-70. (رقم=28)


في الواقع أن النمط الثاني الذي يعقِّد تفسير إحصاءات الجريمة السيبرانية المسجلة لدى الشرطة يتعلق باختلافات في الاستعمال المقارن للجرائم من قِبَل هيئات إنفاذ القانون. فعادة ما تمثل أفعال النفاذ غير المشروع لنظام حاسوبي، والاستيلاء على البيانات الحاسوبية بشكل غير مشروع، والتدخل في البيانات أو النظام بشكل غير مشروع، سلوكا مُتَبَايِنا في القانون. ومع ذلك، فالممارسة العملية توضح أنها غالبا ما قد تندمج في أسلوب سلوك أحادي، مثل "قرصنة" أحد النظم الحاسوبية، نسخ البيانات الحاسوبية من النظام، وإتلاف البيانات في النظام الحاسوبي. فقد يتم تسجيل الشرطة جريمة واحدة أو اثنتين أو ثلاثة بشكل منفصل، اعتمادا على توافر الأدلة، ووصف السلوك، والأولويات السياسية، وقواعد إحْصاء الجريمة.[5] هذا، ويظهر استقراء إحصاءات الجرائم الثلاث المسجلة لدى الشرطة، في فئة

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 55، و57، و58، و68.

[2] See, for instance, Van Dijk, K.J.M., Van Kesteren, J.N., and Smit, P. 2008. *Criminal Victimization in International Perspective. Key findings from the 2004-2005 ICVS and EU ICS*. The Hague: Boom Legal Publishers.

[3] أنظر على سبيل المثال، فيما يتعلق باستغلال الطفل في المواد الإباحية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة. عولمة الجريمة: تقييم تهديد الجريمة المنظمة عبر الوطنية، الفصل 10.

[4] معدلات جرائم القتل المسجلة لدى الشرطة تعرض 100,000 من السكان، بالأحرى من لكل 100,000 من مستخدمي الإنترنت.

[5] تطبيق مبدأ القاعدة الإجرامية، على سبيل المثال، قد يؤدي في تسجيل الجرائم الأكثر جسامة فقط في مَعْرِضِ السلوك. وأشارت نصف البلدان المجيبة إلى أن مبدأ القاعدة الإجرامية قد طُبق لإحصاء الجرائم المسجلة لدى الشرطة. الاستبيان الخاص بالدراسة السؤال رقم 73.

أفعال تمس بالسرية، النزاهة، توافر بيانات حاسوبية أو نظم حاسوب، تباينا كبيرا وفقا للدولة. بيد أنه لا توجد علاقة واضحة موجودة بين الجرائم الثلاثة. فليست هذه هي الحالة، على سبيل المثال، التي تظهر كافة الفئات مستويات متوازية بالتقريب في كل دولة. وبالأحرى، في بعض الدول، فإن الفئة الأولى تعتبر أعلى من الفئتين الأخيرتين. بيد أن في الدول الأخرى، فإن الفئتين الأخيرتين أعلى من الفئة الأولى. كما أن من الملاحظ، أن عددا من الدول ليست لديها إحصاءات متوافرة لكل الفئات الثلاثة. وبينما لا يمكن إثبات أن الاختلافات لا تعكس السمات الحقيقة والأساسية للجريمة، إلى أن هذا التنوع يعتبر من المرجح بشكل كبير أن يبدو متأثرا بالتأثيرات التحقيقية والتسجيل.

وعندما وجه سؤال حول مدى كفاية النظام الحالي لإحصاءات الشرطة لتسجيل أفعال الجريمة السيبرانية، رَأى ثلثا الدول المجيبة بأن أنظمتهم الوطنية ليست كافية.[1] كما أوضحت الدول المجيبة أيضا أن نظم تسجيل إحصاءات الشرطة يمكن تحسينها بعدة طرق. وترد التفاصيل في الجدول في هذه الصفحة.[2]

ورغم هذه القيود، أشارت الدول إلى أهمية إحصاءات الجريمة السيبرانية المسجلة لدى الشرطة لوضع سياسة في مكافحة الجريمة السيبرانية. وذكرت إحدى الدول، على سبيل المثال، أن *"كل أربعة سنوات، تُدمج إحصاءات الشرطة مع المعلومات المعنية بالتأثير والتهديد والتعرض للخطر الذي تسببه الأنواع المختلفة للجريمة، بما في ذلك الجريمة السيبرانية، ويتم تحليل هذه الإحصاءات والمعلومات المدمجة معها في صورة أمن الشرطة المدنية، حيث استخدمت هذه الصورة لتحديد الأولويات في خطة الأمن الوطني للشرطة والعدالة"*.[3]

تحسين إحصاءات الشرطة بشأن الجريمة السيبرانية

- تركيب إشارة في نظام التسجيل لتحديد أحد أركان الجريمة السيبرانية
- إنشاء هيئة مركزية للإبلاغ لسلطات إنفاذ القانون وإحصاءات العدالة الجنائية
- وضع قواعد مُوَحّدة للإحصاء، وبخاصة للأفعال التي تستهدف ضحايا متعددين (مثل "التصيد الاحتيالي")
- مزيد من تطوير أنظمة تصنيف الجريمة لإظْهَار الجريمة السيبرانية

وأبرزت العديد من الدول أنه لا يتعين استخدام إحصاءات الشرطة بشكل منعزل، بالأحرى يجب إدماجها مع مصادر البيانات الأخرى. أيضا أفادت الدول بأن هذا كان الوضع بشكل خاص مع الجريمة السيبرانية، حيث قد لا تتوافق العملية الطويلة لتوليد إحصاءات مسجلة لدى الشرطة مع إيقاع التغير التكنولوجي أو تطور مسار الجريمة السيبرانية. وعلى هذا النحو؛ يتعين إدماج المعلومات الواردة من تقييم الخبراء للتغيرات التكنولوجية الفعلية والمتوقعة، فضلا عن الخبرة بالجرائم

---

[1] الاستبيان الخاص بالدراسة، السؤال رقم 76.

[2] المرجع السابق.

[3] الاستبيان الخاص بالدراسة، السؤال رقم 77

الفعلية والاسترشاد بالسوابق القضائية مع الاتجاهات الإحصائية. هذا، وقد ذكرت دول أخرى أن إحصاءات الجريمة السيبرانية المسجلة لدى الشرطة تعتبر هامة لعمليات الإصلاح التشريعي للإبلاغ، ورفع مستوى الوعي العام بشأن طبيعة الجريمة السيبرانية ونطاقها.[1]

الاستقصاءات السكانية والتجارية

يعتبر، بانتظام، تعزيز الدراسات الاستقصائية بشأن ضحايا الجريمة بمثابة أكثر الطرائق فاعلية لجمع إحصاءات الجريمة. فمن حيث المبدأ، فإن هذه الدراسات تزيل الاشْتِباه "للرقم المعتم" للجريمة التي لم يُبلغ الشرطة عنها من خلال جمع المعلومات مباشرة من السكان من الضحايا المحتملين.[2] وفي نفس الوقت؛ تواجه الدراسات الاستقصائية بشأن ضحايا الجريمة تحديات منهجية، تتضمن الحاجة إلى تحديد دقيق للسكان المستهدفين، لإجراء دراسة استقصائية ملائمة ووضع إطار للعّينات، والتصدي بشكل كاف للدراسات الاستقصائية التي لم يستجب لها.[3] وبالرغم من ذلك؛ إذا تم اعتماد منهجية مِعْيارِيّة وترتيب الأسئلة في الدراسة الاستقصائية، فإن الأخيرة يمكن أن تقدم درجة مناسبة لإمكانية المقارنة عبر الحدود الوطنية.[4]

ومن الملاحظ؛ أن الدراسات الاستقصائية الدولية والإقليمية بشأن ضحايا الجرائم ليس لديها حتى الآن أسئلة مُوَحّدة ومَدْمُوجة بشكل منظّم تتعلق بالجريمة السيبرانية. بيد أن بعض الدراسات الاستقصائية السكانية الوطنية تتناول "التجارب السلبية عند استعمال الإنترنت"،[5] أو "وقائع البرمجيات الخبيثة"،[6] أو "استخدام الحاسوب في الأعمال ذات الصلة بالتهديد بالإيذاء أو الاعتداء أو "الاحتيال عبر الإنترنت".[7] وفي هذا الصدد أيضا، تتناول إحدى الدراسات الاستقصائية الوطنية الأخرى الجرائم التي قد تنطوي على النظم الحاسوبية أو البيانات الحاسوبية – أو غيرها – بما في ذلك، "انتحال الشخصية"،[8] و"استنساخ البطاقات المصرفية".[9] هذا، وقد تضمنت الدراسات الاستقصائية الإقليمية أسئلة أيضا بشأن "استلام رسائل إلكترونية احتيالية تتضمن طلبا للمال". "الاحتيال عبر الإنترنت متى لم يتم تسليم السلع المشتراة، والتي قد تكون مُقَلّدة أو غير ذلك حسبما أوعز إليه"، و"التعرض لِمواد عرضيّا تحرض على الكراهية العرقية أو التطرف الديني".[10] وفي هذا الشأن أيضا، تتضمن

---

[1] المرجع السابق.

[2] للاطلاع على نظرة شاملة على المنهجية المستخدمة في الدراسة الاسقصائية بشأن ضحاي الجريمة، انظر مكتب الأمم المتحدة المعني بالمخدرات والجريمة واللجنة الاقتصادية لأوروبا 2010. دليل الدراسات الاستقصائية بشأن ضحايا الجرائم

[3] المرجع السابق

[4] See, for example, Van Dijk, K.J.M., Van Kesteren, J.N., and Smit, P. 2008. *Criminal Victimization in International Perspective. Key findings from the 2004-2005 ICVS and EU ICS*. The Hague: Boom Legal Publishers.

[5] وزارة الداخلية البريطانية. 2012. جرائم الكراهية والأمن السيبراني وممارسة الجريمة بين الأطفال: نتائج الدراسة الاستقصائية البريطانية 2010/11: المجلد التكميلي 3، الجريمة في انجلترا وويلز 2010/11.

[6] AusCert. 2008. *Home Users Computer Security Survey 2008*.

[7] Hong Kong UNICVS. 2010. *Final Report of the 2006 Hong Kong UNICVS*.

[8] وزارة العدل الأمريكية، مكتب إحصاءات وزارة العدل 2008. الدراسة الاستقصائية الوطنية التكميلية بشأن ضحايا سرقة الهوية 2008.

[9] INEGI. 2012. *Encuesta Nacional de Victimizacíon y Percepcíon sobre Seguridad Pública 2012 (ENVIPE), Cuestionario Principal*

[10] European Commission. 2012. *Special Eurobarometer 390: Cybersecurity*

الدراسات الاستقصائية الدولية، مثل الدراسة الاستقصائية الدولية لضحايا الجريمة،[1] سؤالا واحدا فقط مباشرا يتعلق بالجريمة السيبرانية بشأن التعرض لاحتيال أثناء التسوق عبر الإنترنت. وقد طلبت الدراسات الاستقصائية السكانية التي أعدها القطاع الخاص "ردا بشأن البريد الإلكتروني الوهمي أو المواقع الإلكترونية الكاذِبة والتي تم من خلالها الحصول على تفاصيل شخصية"، و"البلطجة أو التعقب أو جرائم كراهية أو تحرش عبر الإنترنت"،[2] و"اختراق حساب البريد الإلكتروني أو الملف التعريفي على شبكات التواصل الاجتماعي"، "والإيذاء الاحتيالي بتزوير بطاقات الائتمان"،[3] و"سرقة البيانات التي ترتكب عبر شبكة الإنترنت".[4]

وقامت كيانات القطاع الخاص بإجراء مزيد من الدراسات الاستقصائية بشأن ضحايا الجريمة السيبرانية التي تعاني منها الشركات التجارية.[5] بينما قد تستخدم بعض من هذه الدراسات الاستقصائية أحد أطر العّينات الإحصائية، إلا أن أغلبية الدراسات تعتبر دراسات استقصائية معنية بالعملاء، أو اختيار "المبلغين الأساسيين". وفي هذا الصدد أيضا؛ قام عدد قليل من الحكومات الوطنية بإجراء دراسات استقصائية تناولت إيذاء الشركات.[6] بالإضافة إلى ذلك؛ قام المكتب الإحصائي للجماعات الأوروبية مؤخرا بإعداد دراسة استقصائية بشأن استخدام تكنولوجيا المعلومات والاتصالات في الشركات، تناولت المسائل المتعلقة بالجريمة السيبرانية والأمن السيبراني في أحد الوحدات المخصصة.[7] وقد استعملت الأسئلة الواردة في الدراسة الاستقصائية التجارية لغة "الحادث الأمني" لتغطية مجموعة واسعة من أفعال الجريمة السيبرانية، بما في ذلك؛ النفاذ غير المشروع من قِبَل اختراق نظام حاسوبي دخيل أو القرصنة أو التدخل في البيانات/النظام في شكل عدوى البرمجيات الخبيثة أو هجمات حجب الخدمة الموزعة، أو استعمال الحاسوب في أعمال الاحتيال من قِبَل "المطلعين على أمور الشركة"، أو الحصول على بيانات حاسوبية بشكل غير قانوني في شكل "اختراق للبيانات".

فمن الملاحظ أنه يوجد تباين كبير في استعمال المصطلحات، وفي طريقة طرح الأسئلة وتكرار إدْراج الأسئلة المتعلقة بالجريمة السيبرانية في الدراسات الإحصائية المعنية بضحايا الجرائم. فليس من المألوف للأسئلة المعنية بالجريمة السيبرانية أن يتم تضمينها "كوحدة" خاصة للدراسات الإحصائية الدورية المعنية بضحايا الجرائم، مما

---

[1] لمزيد من الدراسات الاستقصائية الدولية بشأن ضحايا الجرائم، انظر: http://www.crimevictimsurvey.eu and http://rechten.uvt.nl/icvs

[2] تضمنت الاستبيان الملحق بالدراسة الاستقصائية الدولية بشأن ضحاي الجريم متابعة للمشاركين في الاستبيان الذين أشاروا إلى أنهم كانوا أحد ضحايا الاحتيال على المستهلكين. والسؤال كان: كيف حدث هذا الاحتيال؟ هل وقع ذلك اثناء [التسوق عبر الإنترنت؟]..

[3] Symantec. 2012. *Norton Cybercrime Report 2012*

[4] McAfee/National Cybersecurity Alliance. 2012. *Online Safety Survey*

[5] See, for example, Computer Security Institute. 2011. *CSI Computer Crime and Security Survey 2010/2011*; PricewaterhouseCoopers. 2012. *Global State of Information Security Survey*; Ponemon/Check Point Software Technologies. 2012. *The Impact of Cybercrime on Business*; and Ponemon/HP Enterprise Security. 2012. *Cost of Cybercrime Study 2012*.

[6] أنظر على سبيل المثال؛ وزارة العدل الأمريكية، مكت إحصاءات وزارة العدل. 2006. دراسة استقصائية وطنية بشأن حوادث الأمن الالكتروني، انظر أيضا المعهد الأسترالي للدراسات الجنائية. 2009. تقييم الشركات التجارية لاستخدام الأمن الالكتروني: دراسة استقصائية وطنية.

[7] المكتب الإحصائي للجماعات الأوروبية. 2011. دراسة استقصائية بشأن استخدام تكنولوجيا المعلومات والاتصالات والتجارة الإلكترونية في المؤسسات. متاح على الرباط التالي:
http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

يجعل من الصعب إيجاد هيكل زمني للبيانات المتسلسلة. وفي حين أن بعضا من الدراسات الاستقصائية تتضمن الدول النامية،[1] إلا أن التركيز يتم غالبا على الدولة المتقدمة، مما ينتج عن ذلك حاجة ملحة لبيانات استقصائية من جزء كبير من العالم. ففي أثناء جمع المعلومات الخاصة بهذه الدراسة، فإن عددا قليلا جدا من الدول التي كانت قادرة على تقديم معلومات بشأن الدراسات الاستقصائية السكانية أو الدراسات الاستقصائية التجارية المتعلقة بالجريمة السيبرانية.[2] وإذا كانت البيانات الاستقصائية متوافرة، إلا أنها تخضع إلى عدد من الانتقادات، بما في ذلك الصعوبة في الحصول على إحدى العينات والتي تمثل ليس فقط تعرض السكان للخطر وإنما أيضا الخسائر التي تسببها الجريمة السيبرانية ويتحملها السكان.[3]

ويعتبر المزيد من تطور المنهجية وهيكل أسئلة الدراسة الاستقصائية من الأمور الحيوية للجهود المستقبلية في قياس طبيعة وسياق الجريمة السيبرانية. وبينما تعتبر الجريمة السيبرانية في بعض النواحي من الجرائم الصعبة عند قياسها نظرا لعدم وجود العوامل التعريفية فضلا عن الافتقار إلى الوعي، إلى جانب ذلك، فإن السوابق القضائية الموجودة – لتوفيق منهجيات الدراسات الاستقصائية المعنية بالإيذاء – تؤدي إلى صعوبة أخرى في قياس الجرائم، مثل العنف ضد المرأة.[4] بالإضافة إلى ذلك؛ فقد ركزت التطورات الحديثة في الدراسات الاستقصائية الدولية المعنية بضحايا الجريمة على تمحيص منهجيات الدراسات الاستقصائية للإنترنت،[5] كخطوة هامة في حالة إذا كان السكان المعنيون هم من "مستخدمي الإنترنت". وتبرز إحدى خرائط الطريق الحديثة لتحسين إحصاءات الجريمة على المستوى الوطني والدولي أهمية تطوير الدراسات الاستقصائية وتمحيصها لجمع البيانات بشأن أشكال محددة من الجريمة السيبرانية.[6] وفي هذه الدراسة؛ تعتبر البيانات الإحصائية الواردة من إحدى الدراسات الاستقصائية السكانية للمقارنة عبر الحدود الوطنية –القليلة– مستخدمة في القسم الخاص بـ "الصورة العالمية للجريمة السيبرانية".

---

1 See, for example, Symantec. 2012. *Norton Cybercrime Report 2012* (includes South Africa), and PricewaterhouseCoopers. 2011. *Cybercrime: Protecting against the Growing Threat. Global Economic Crime Survey* (covers 78 countries, including 13 in Africa).

2 الاستبيان الخاص بالدراسة، السؤال رقم 10

3 Florêncio, D., and Herley, C. 2011. *Sex, Lies and Cybercrime Surveys*. Available at: http://research.microsoft.com/pubs/149886/sexliesandcybercrimesurveys.pdf

4 See Johnson, H., and Nevala. S. 2010. *International Violence Against Women Survey (IVAWS)*.

5 See http://crimevictimsurvey.eu

6 اللجنة الإحصائية للأمم المتحدة. 2012. تقرير المعهد الوطني المكسيكي للإحصاء والجغرافيا، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة بشأن إحصاءات الجريمة: خارطة طريق لتحسين إحصاءات الجريمة على المستوى الوطني والدولي. E/CN.3/2013/11 . 19-كانون الأول/ديسمبر 2012.

المبادرات الخاصة ببلاغات الضحايا

غالبا ما يفضل ضحايا الجريمة السيبرانية تقديم بلاغ عن الفعل الإجرامي السيبراني إلى أحد مراكز الإبلاغ عن الجريمة السيبرانية، مثل أحد المواقع الإلكترونية أو الخطوط الساخنة أو بالأحرى من خلال قنوات الشرطة التقليدية (بالرغم من وجود روابط وثيقة عادة بين مراكز الإبلاغ وسلطات إنفاذ القانون). وتوجد هذه المبادرات الخاصة بالإبلاغ في عدد من الدول، ومنها جنوب آسيا،[1] أمريكا الوسطى،[2] وأوروبا الغربية،[3] وأمريكا الشمالية.[4] وتعتبر المواقع الإلكترونية المعنية بالإبلاغ الذاتي من قبل الضحية موجودة أيضا بشكل متزايد في عدد من الدول النامية، مثل دول غرب أفريقيا.[5] وعلى غرار إحصاءات الشرطة، فإن البيانات المنبثقة عن البلاغات المقدمة إلى المراكز بشأن الجريمة السيبرانية تعاني هي الأخرى من "الرقم المعتم" للجرائم المجهولة. ولذلك تعتبر هذه البيانات غير مناسبة للاستخدام في مقارنات مستويات الجريمة السيبرانية عبر الحدود الوطنية. حتى الاتجاهات في الشكاوى قد تكونُ مسَيّرة إلى حد كبير طبقا لمستويات وعي الضحايا إلى جانب الأحداث الأساسية.[6]

وبالرغم من ذلك؛ فإن الإحصاءات المنبثقة من آليات إبلاغ الضحايا يمكن أن يقدم استدلالات بشأن توزيع أفعال الجريمة السيبرانية داخل إحدى الدول. وقد تظهر الإحصاءات، على سبيل المثال، معالم مثل الأنماط الرئيسية لاستعمال الحاسوب في الاحتيال المبلغ عنه، توزيع الفئة العمرية للضحايا وجنسهم، أو طبيعة المحتوى غير القانوني المبلغ عنه.[7] كما هو الحال في الإحصاءات المسجلة لدى الشرطة، فإن مقارنة البيانات الواردة من مبادرات بلاغات الضحايا يمكن تعزيزها من خلال وضع تصنيفات موحدة لأفعال الجريمة السيبرانية.

المعلومات الخاصة بالأمن السيبراني القائم على التكنولوجيا

ربما تعتبر أفعال الجريمة السيبرانية متفردة بين الجرائم بشكل عام، في وجود تدابير وقائية ممتدة قائمة على التكنولوجيا، بما في ذلك منتجات مكافحة الفيروسات وأمن الشبكات، بجانب برامج الحماية.[8] ويقوم دور هذه المنتجات عادة على المسح الضوئي، وتحديد وتنقية "التوقيعات" الإلكترونية المحددة. هذا، وقد تكون هذه

---

[1] See http://www.cybercellindia.com/#

[2] See http://fiscalia.chihuahua.gob.mx/intro/?page_id=3029

[3] See https://www.meldpuntcybercrime.nl/english_information.html; http://www.cybercrime.admin.ch/content/kobik/en/home/meldeformular.html; and http://www.actionfraud.police.uk/home

[4] See http://www.ic3.gov/default.aspx

[5] See http://cybercrime.interieur.gouv.ci/?q=node/4

[6] تشير التقارير السنوية لمركز الإبلاغ IC3 بالولايات المتحدة الأمريكية، على سبيل المثال، إلى زيادة مطردة من عام 2000 إلى 2009 حتى آخر تسوية في 2010 إلى 2011. أنظر: مركز شكاوى جرائم الإنترنت. 2011. تقرير جرائم الانترنت 2011. وعلى النقيض من ذلك، فإن عدد البلاغات التي تلقاها مركز البلاغات السويسري يشير إلى انخفاض من 2007 إلى 2011. أنظر:
Service de Coordination de la Lutte Contre la Criminalité sur Internet (SCOCI) 2011. *Rapport Annuel 2011*. Awareness of reporting mechanisms may increase over time or decrease over time, depending on factors such as the degree and consistency of publicity accompanying the mechanism.

[7] المرجع السابق.

[8] See OECD. 2002. *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks Towards a Culture of Security*. 25 July 2002 - C(2002)131/FINAL

المنتجات قائمة على المحتوى أو قائمة على حركة المرور، مثل المراسلات من أو إلى "القائمة السوداء" لبرتوكولات الإنترنت".[1] ويتضمن العديد من المنتجات أيضا الكشف الإرشادي والذي من شأنه أن يقوم بفحص مسار الملفات المشتبه بها وظروف الاتصالات المحددة سلفا. وبالتالي، فإن سجلات الحركة المنشأة من قبل منتجات أمنية قائمة على التكنولوجيا يمكنها تقييد مجموعة فرعية من محتوى الحاسوب ومجريات حركة المرور التي قد تتوافق مع أحد مكونات أفعال الجريمة السيبرانية، وذلك في بعض الحالات. ومن ناحية أخرى؛ فإن الشروع في – أو اكتمال – ارتكاب أفعال النفاذ غير المشروع إلى نظام حاسوبي أو التدخل غير المشروع في بيانات حاسوبية أو أحد النظم الحاسوبية قد يتم كشفه، على سبيل المثال، من خلال استجابة هذه المنتجات. هذا، ويعتبر إنذارا ضد السرقة المنزلية والتي يكشف عن الأحداث عند الأبواب والنوافذ المنزلية بمثابة مُضَاهَاة ضَعِيفة، نظرا لأن حقيقة تشغيل أحد الإنذارات لا يعني بالضرورة أن هناك جريمة قد تم ارتكابها، وبالرغم من ذلك؛ فإن نسبة محددة من الجرائم قد تستدعي تشغيل التنبيه.

وجدير بالذكر؛ أن إحدى ميزات منتجات الأمن السيبراني القائمة على التكنولوجيا تتمثل في أن أعدادا كبيرة من "إنذارات السرقة" قد تبلغ كأحداث مسجلة إلى أحد المواقع المركزية – مما يسمح بإعْداد إحصاءات إجمالية للأمن السيبراني. والعديد من مقدمي خدمات الأمن السيبراني من القطاع الخاص يعد تقارير مؤسسة على هذه الإحصاءات.[2] وغالبا ما يستخدم مقدمو خدمات الأمن السيبراني، مع ذلك، تعريفات مختلفة بشكل واضح: أساليب العَدّ، والسلاسل الزمنية، والتغطية الجغرافية، وعروض البيانات.[3] وكنتيجة لذلك، فإن مقارنة الإحصاءات عبر "تقارير التهديد" التي يعدها القطاع الخاص تشكل تحديا إلى أبعد حد. وفي بعض الحالات؛ تُقدم هذه البيانات باعتبارها إحصاءات بشأن "الجريمة السيبرانية".[4] ومع ذلك، فإنه من الملائم عرض المعلومات الخاصة بالأمن السيبراني القائم على التكنولوجيا باعتبارها ذات دَلَالَة بظاهرة الأمن السيبراني والتي قد تشكل — أو لا تشكل – أفعال الجريمة السيبرانية.

وبالرغم من ذلك؛ فإن المعلومات بشأن "التهديدات" الإلكترونية من منتجات الأمن السيبراني يمكن استخدامها، مع توخي بعض الحذر، للمساعدة في فهم الأنماط الواسعة في الفئة الأولى للجرائم السيبرانية: أفعال ضد السرية، النزاهة، توافر بيانات حاسوبية أو نظم حاسوب. فهذه المعلومات يمكن أن يكون لديها بشكل خاص درجة عالية من القابلية للمقارنة عبر الوطنية – استعمال ذات البيانات التي تم جمعها ومعالجة النظام –

[1] Callanan, C., Gercke, M., De Marco, E., and Dries-Ziekenheiner, H. 2009. *Study on Internet blocking, balancing cybercrime responses in democratic societies.* Aconite Internet Solutions, October 2009.

[2] See for example AVG. 2011. *Community Powered Threat Report 2012*; Cisco 2011. *Cisco Threat Report 2011*; IBM. 2011. *IBM Trend and Risk Report 2011*; McAfee 2012. *McAfee Threats Report. First Quarter 2012*; Microsoft. 2011. *Microsoft Security Intelligence Report. Volume 12*; PandaLabs. 2012. *PandaLabs Quarterly Report. April-June 2012*; Sophos. 2012. *Security Threat Report 2012*; Symantec. 2011. *Internet Security Threat Report. 2011 Trends, Volume 17*; Total Defense. 2011. *Threat Report: End of Year 2011*; and Trend Micro. 2011. *TrendLabs Annual Security Roundup.*

[3] *Ibid.* See also PricewaterhouseCoopers. 2012. E*ye of the storm. Key findings from the 2012 Global State of Information Security Survey; World Economic Forum.* 2012. Global Risks 2012, 7th ed.

[4] See, among others, Symantec. 2011. *Internet Security Threat Report. 2011 Trends, Volume 17.*

حيث من المرجح تركيب نفس المنتج في أنظمة حاسوب متعددة في مختلف الدول. وتستخدم هذه الدارسة المعلومات الخاصة بالأمن السيبراني القائم على التكنولوجيا لتوصيف أداة معينة، شبكات الروبوت، التي استخدمت غالبا في أفعال الجريمة السيبرانية.

وأخيرا، أفادت غالبية الدول بعدم كفاية إحصاءات الشرطة المعنية بتسجيل أفعال الجريمة السيبرانية. وبينما ذكرت أغلبية قليلة من الدول الأوروبية أن إحصاءات الشرطة تُمكّن بشكل كاف من القبض على مرتكبي أفعال الجريمة السيبرانية، وعلى النقيض من ذلك، ففي جميع المناطق الأخرى، أفادت أغلبية كبيرة من الدول بأن إحصاءات الشرطة لا تعتبر كافية لتسجيل تلك الحالات.

الملحق الثالث: الأحكام الواردة في الصكوك الدولية والإقليمية

التعاريف	الاتحاد الأفريقي[1]	السوق المشتركة لشرق وجنوب أفريقيا (الكوميسا)[2]	الكومنولث[3]	كومنولث الدول المستقلة[4]	مجلس أوروبا (اتفاقية بودابست والبروتوكول الاختياري)[5]	مجلس أوروبا (اتفاقية لانزروت)[6]	الجماعة الاقتصادية لدول غرب أفريقيا[7]	الاتحاد الأوروبي (القرار الإطاري JHA/2005/222)[8]	الاتحاد الأوروبي (المشروع التوجيهي 2010/073)[9]	الاتحاد الأوروبي (القرار الإطاري JHA/2001/413)[10]	الاتحاد الأوروبي (التوجيه EU/92/2011)[11]	الاتحاد الدولي للاتصالات (ITU)/CARICOM/CTU (نصوص تشريعية نموذجية)[12]	الاتفاقية العربية لمكافحة جرائم المعلومات[13]	القانون النموذجي العربي بشأن مكافحة الجريمة السيبرانية[14]	منظمة شنغهاي للتعاون[15]	الأمم المتحدة (اتفاقية حقوق الطفل–البروتوكول الاختياري)[16]
نظام حاسوبي/معلوماتي	المادة 1(3-6)	المواد 1/ب 1/هـ 1/ن	المادة 3		المادة 1/أ		المادة 1	المادة 1/أ	المادة 2/أ			المواد 5/3 *6/2 17/2*	المادة 2/1 2/5	المادة 1		
شبكة حاسوبية/معلوماتية		المادة 1/ف											المادة 2/6	المادة 1		
جهاز/وسائط التخزين			المادة 3									المواد 7/3 9/3				
البنية التحتية الحيوية		المادة 1/ز										المادة 8/3			المادة 1	
البيانات/المعلومات الحاسوبية (بما فيها برامج الحاسوب)	المادة 2/1	المواد 1/ج 1/د 2/ي	المادة 3	المادة 1/ب	المادة 1/ب		المادة 1	المادة 1/ب	المادة 1/ب			المواد 6/3 *9/2	المادة 2/3 2/4	المادة 1		
التسجيل الإلكتروني		المادة 1/ى	المادة *2									المواد 15/2*				
المشترك/حركة مرور/بيانات المحتوى/معلومات		المواد 1/و 1/ش 1/ت	المادة 3		المادة 1/ب 18							المواد 18/3 *7/2 27/2* 28/2*	المادة 2/9			
المراسلات/البريد الالكتروني	المادة 1/1	المادة 1/م					المادة 1					14/2*				
برمجيات ضارة/خبيثة		المادة 1/ص		المادة 1/ج												
مقدمي خدمة (الإنترنت)		المادة 1/ر	المادة 3		المادة 1/ج							المواد 1/3 2/3 11/3 17/3	المادة 2/2			
الطفل/القاصر	المادة 4/1		المادة 10/3		المادة 3/9	المادة 3	المادة 1				المادة 3/3	المادة 3/3				المادة 3/ج
الجريمة السيبرانية/الجريمة الحاسوبية					المادة 1 (أ)										الملحق 1	

التجريم	الاتحاد الأفريقي[1]	السوق المشتركة لشرق وجنوب أفريقيا[2]	الكومنولث[3]	كومنولث اتحاد الدول المستقلة[4]	مجلس أوروبا (اتفاقية بودابست والبروتوكول الاختياري)[5]	مجلس أوروبا (اتفاقية لانزروات)[6]	الجماعة الاقتصادية لدول غرب أفريقيا[7]	الاتحاد الأوروبي (القرار الإطاري JHA/2005/222)[8]	الاتحاد الأوروبي (المشروع التوجيهي 2010/073)[9]	الاتحاد الأوروبي (القرار الإطاري JHA/2001/413)[10]	الاتحاد الأوروبي (التوجيه EU/92/2011)[11]	الاتحاد الدولي للاتصالات (ITU)/CARICOM/CTU[12] (نصوص تشريعية نموذجية)	الاتفاقية العربية لمكافحة جرائم المعلومات[13]	القانون النموذجي العربي بشأن مكافحة الجريمة السيبرانية[14]	منظمة شنغهاي للتعاون[15]	الأمم المتحدة (اتفاقية حقوق الطفل–البروتوكول الاختياري)[16]
النفاذ غير المشروع إلى أحد نظم الحاسوب	المواد 15 16	المواد 18 19	المواد 5 7		المادة 2		المواد 2 3	المادة 2/1	المادة 3			المواد 4 5	المادة 6	المواد 3 5 15 22		
النفاذ واعتراض البيانات الحاسوبية والحصول عليها بشكل غير مشروع	المادة 23	المواد 19 21	المواد 5 8	المادة 1/3 (أ)	المواد 2 3		المادة 6		المادة 6			المواد 6 8	المواد 6 7 18	المواد 3 8		
التدخل غير القانوني في البيانات الحاسوبية	المواد 19 20 24	المواد 20 22(أ)	المادة 6	المادة 1/3 (ج)	المادة 4		المواد 5 7	المادة 4	المادة 5	المادة 3		المادة 7	المادة 8	المادة 6		
التدخل غير القانوني في النظام الحاسوبي	المادة 18 19	المادة 22/أ	المادة 7	المادة 1/3 (ج)	المادة 5		المادة 5	المادة 3	المادة 4	المادة 3		المادة 9	المادة 6	المادة 7		
أدوات إساءة استخدام الحاسوب	المواد 22 22 (ج)	(0) 22	المادة 6	أ 1(1) –ب	المادة 6		المادة 12	المادة 5	المادة 7	المادة 4		المادة 10	المادة 9			
انتهاك الخصوصية وتدابير حماية البيانات	المواد 27			المادة 3			المادة 13				المادة 15 (أ 1) (1					
استعمال الحاسوب في التزوير	المواد 24 25	المادة ,2			المادة 7		المادة 8			المواد 2 4		المادة 11	المواد 10 18	المادة 4		
استعمال الحاسوب في الاحتيال	المواد 25 26 41	المواد 24/أ 24/ب			المادة 8		المواد 9 10 23			المادة 2 4		المادة 12	المادة 11	المواد 10 11 12		
جرائم وسائط الدفع الإلكتروني										المادة 2			المادة 18	المادة 11		
الجرائم المتعلقة بالهوية												المادة 14				

1 التوجيه 2002/58/EC (لا يعتبر شرطا لازما للتجريم)

الجرائم المتعلقة بحقوق المؤلف والنشر وتقليد العلامات التجارية				المواد 1/3 (د)	المادة 10								المادة 17	المادة 14		
البريد الإلكتروني الطفيلي		المادة 19/ز									المادة 13 3(2)	المادة 15				
أعمال الحاسوب المتعلقة بالتحرش والابتزاز وأعمال التسبب في الضرر الشخص	المواد 40 41	المادة 25										المادة 15		المادة 9		
استعمال الحاسوب في الأعمال التي تنطوي على عنصرية وكراهية الأجانب	المواد 34 35 36				المواد 3 4 5 OP		المواد 18 19 20									
الأعمال ذات الصلة بالحاسوب المتعلقة بإنكار جرائم الإبادة الجماعية أو الجرائم ضد الانسانية	المادة 37				المادة 6 OP		المادة 21									
استعمال الحاسوب في انتاج أو توزيع أو حيازة مواد إباحية عن الأطفال	المواد 29 30 31 32		المادة 10		المادة 9	المادة 20	المادة 14 15 16 17				المادة 5	المادة 13	المادة 12			المادة 3
استعمال الحاسوب في استمالة أو إغواء الأطفال						المادة 23					المادة 6					
استعمال الحاسوب في دعم الإرهاب	المادة 40	المواد 18 19 20/أ											المادة 15	المادة 21		
استعمال الحاسوب في جرائم غسل الأموال													المادة 15	المادة 19		
استعمال الحاسوب في الاتجار غير المشروع													المادة 16	المواد 17 18		
استعمال الحاسوب في جرائم ضد الأمن العام والأخلاق والنظام العام							المواد 14 15 16 17						المواد 12 13 14 15	المواد 13 16 20		

الجرائم المتعلقة بتحقيقات هيئات إنفاذ القانون	المادة 54		المواد 13 21		المواد 3/16 3/20 3/21							المادة 17	المواد /23 3 /28 3 /29 3			
الظروف المشددة للعقوبة للجرائم التقليدية المرتكبة باستخدام نظام حاسوبي	المادة 40						المادة 22						المادة 21			
الشروع والمساعدة والتحريض		المادة 26			المادة 11 OP7	المادة 24			المادة 8							
مسؤولية الشركات		المادة 27			المادة 12	المادة 26										

الصلاحيات الإجرائية	الاتحاد الأفريقي [1]	السوق المشتركة لشرق أفريقيا والجنوب الأفريقي [2]	الكومنولث [3]	كومنولث اتحاد الدول المستقلة [4]	مجلس أوروبا (اتفاقية بودابست والبروتوكول الاختياري) [5]	مجلس أوروبا (اتفاقية لانزروات) [6]	الجماعة الاقتصادية لدول غرب أفريقيا [7]	الاتحاد الأوروبي (القرار الإطاري JHA/2005/222) [8]	الاتحاد الأوروبي (المشروع التوجيهي 2010/073) [9]	الاتحاد الأوروبي (القرار الإطاري JHA/2001/413) [10]	الاتحاد الأوروبي (التوجيه EU/92/2011) [11]	الاتحاد الدولي للاتصالات (ITU)/CTU/CARICOM (نصوص تشريعية نموذجية) [12]	الاتفاقية العربية لمكافحة جرائم المعلومات [13]	القانون النموذجي العربي بشأن مكافحة الجريمة السيبرانية [14]	منظمة شنغهاي للتعاون [15]	الأمم المتحدة (اتفاقية حقوق الطفل–البروتوكول الاختياري) [16]
البحث عن أجهزة الحاسوب أو البيانات	المادة 50	المواد أ/37 ب/37	المادة 12		المواد 1/19 2/19		المادة 33					المادة 20	المادة 26			
مصادرة أجهزة الحاسوب أو البيانات	المادة 51	المادة ج/37	المواد 12 14		المادة 3/19		المادة 33					المادة 20	المادة 1/27			
الأمر الخاص بالبيانات الحاسوبية المخزنة		المادة أ/36	المادة 15		المادة 1/18 أ							المادة أ/22	المادة 1/25			
الأمر الخاص بمعلومات أحد المشتركين		المادة ب/36			المادة 1/18 ب							المادة ب/22	المادة 2/25			
الأمر الخاص بحركة البيانات المخزنة		المادة أ/34 2	المادة 16		المادة 1/17 ب							المادة 24	المادة 24			
الوقت الحقيقي لجمع حركة البيانات		المادة 38	المادة 19		المادة 20							المادة 25	المادة 28			

الوقت الحقيقي لجمع محتوى البيانات	المادة 55	المادة 39	المادة 18		المادة 21							المادة 26	المادة 29			
التحفظ المعجل على البيانات الحاسوبية	المادة 53	المواد 33- 34/أ (1) 35	المادة 17		المادة 16 1/17 أ		المادة 35					المادة 23	المادة 2/23			
استعمال أدوات التحليل الجنائي عن بُعد						المادة 5/30					المادة 15	المادة 27				
الوصول للبيانات الحاسوبية عبر الحدود الوطنية		المادة 49/ب			المادة 32/ب								المادة 2/40			
تقديم المساعدة		المادة 37/ب	المادة 13		المادة 4/19							المادة 21	المادة 2/27			
الاحتفاظ بالبيانات الحاسوبية		المواد 29 30 31								المواد 3 6						

الأدلة الإلكترونية	الاتحاد الأفريقي[1]	السوق المشتركة لشرق وجنوب أفريقيا[2]	الكومنولث[3]	كومنولث اتحاد الدول المستقلة[4]	مجلس أوروبا (اتفاقية بودابست والبروتوكول الاختياري)[5]	مجلس أوروبا (اتفاقية لانزوروت)[6]	الجماعة الاقتصادية لدول غرب أفريقيا[7]	الاتحاد الأوروبي (القرار الإطاري JHA/2005/222)[8]	الاتحاد الأوروبي (المشروع التوجيهي 2010/073)[9]	الاتحاد الأوروبي (القرار الإطاري JHA/2001/413)[10]	الاتحاد الأوروبي (التوجيه EU/92/2011)[11]	الاتحاد الدولي للاتصالات (ITU)/CARICOM/CTU (نصوص تشريعية نموذجية)[12]	الاتفاقية العربية لمكافحة جرائم المعلومات[13]	القانون النموذجي العربي بشأن مكافحة الجريمة السيبرانية[14]	منظمة شنغهاي للتعاون[15]	الأمم المتحدة (اتفاقية حقوق الطفل – البروتوكول الاختياري)[16]
مقبولية الأدلة/السجلات الإلكترونية	المادة 24/1	المادة 5/أ	المواد 20 3* 11*				المادة 34					المواد 5* 1/7* 12*				
مقبولية التوقيع الإلكتروني			المادة 12									المادة 14*				
عبء الإثبات			المادة 5*									المادة 9*				
قاعدة أفضل دليل			المادة 6*									المادة 6*				
المطبوعات باعتبارها أفضل دليل												المادة 8*				
افتراض سلامة الدليل			المادة 7*									المادة 2/7*				

الولاية القضائية	الاتحاد الأفريقي[1]	السوق المشتركة لشرق أفريقيا والجنوب الأفريقي[2]	الكومنولث[3]	كومنولث اتحاد الدول المستقلة[4]	مجلس أوروبا (اتفاقية بودابست والبروتوكول الاختياري)[5]	مجلس أوروبا (اتفاقية لانزاروت)[6]	الجماعة الاقتصادية لدول غرب أفريقيا[7]	الاتحاد الأوروبي (القرار الإطاري JHA/2005/222)[8]	الاتحاد الأوروبي (المشروع التوجيهي 2010/073)[9]	الاتحاد الأوروبي (القرار الإطاري JHA/2001/413)[10]	الاتحاد الأوروبي (التوجيه EU/92/2011)[11]	الاتحاد الدولي للاتصالات CTU/CARICOM/(ITU) (نصوص)[12]	الاتفاقية العربية لمكافحة جرائم المعلومات[13]	القانون النموذجي العربي بشأن مكافحة الجريمة السيبرانية[14]	منظمة شنغهاي للتعاون[15]	الأمم المتحدة (اتفاقية حقوق الطفل–البروتوكول الاختياري)[16]
الأدلة بشأن معايير التسجيل/التحفظ			المادة 8*									المادة 10*				
الأدلة/السجلات الإلكترونية من دول أخرى ووثائق أجنبية												المواد 16* 17*				
مبدأ الإقليمية		المادة 40 1/أ	المادة 4/أ		المادة 22 1/أ	المادة 25 1/أ		المادة 10 1/أ	المادة 13 1/أ	المادة 9 1/أ	المادة 17 1/أ	المادة 19/أ	المادة 30 1/أ			المادة 1/4
استعمال أحد النظم/البيانات الحاسوبية الموجودة داخل الإقليم		المادة 40 2/أ														
التوجيه ضد استعمال أحد النظم/البيانات الحاسوبية الموجودة داخل الإقليم		المادة 40 3/أ						المادة 10 2/ب	المادة 13 2/ب							
مبدأ المواطنة (الجاني)		المادة 40/ج	المادة 4/ج د		المادة 22 1/د	المادة 25 1/د		المادة 10 1/ب	المادة 13 1/ب	المادة 6 1/ب	المادة 17 1/ب	المادة 19/ج	المادة 30 1/د			المادة 4 2/أ
مبدأ المواطنة (المجني عليه)						المادة 2/25					المادة 17 2/أ					المادة 4 2/ب
مبدأ الإقامة المعتادة						المادة2 1/5 2/25 3/25			المادة 13 1/ب		المادة 17 2/أ 2/ج					المادة 4 2/أ
الشخص الاعتباري–مبدأ الدمج								المادة 10 1/ج	المادة 13 1/ج	المادة 9 1/ج	المادة 17 2/ب					
مبدأ مصلحة الدولة													المادة 30 1/ج	المادة 26		

الاختصاص عند رفض التسليم		المادة 40/د			المادة 3/22	المادة 7/25		المادة 3/10		المادة 1/10			المادة 2/30			المادة 3/4
السفن والطائرات		المادة 40/ب			المادة 22 1/ب ج	المادة 25 1/ج							المادة 30			المادة 1/4
التجريم المزدوج			المادة 4/د		المادة 22 1/د					المادة 9 1/ب			المادة 30 1/د			
الاختصاص المشترك		المادة 10/ج			المادة 5/22	المادة 8/25		المادة 4/10					المادة 3/30			
محل وقوع الجريمة		المادة 1/40										المادة 3/17				

التعاون الدولي	الاتحاد الأفريقي[1]	السوق المشتركة لشرق أفريقيا والجنوب الأفريقي[2]	الكومنولث[3]	كومنولث اتحاد الدول المستقلة[4]	مجلس أوروبا (اتفاقية بودابست والبرتوكول الاختياري)[5]	مجلس أوروبا (اتفاقية لانزروات)[6]	الجماعة الاقتصادية لدول غرب أفريقيا[7]	الاتحاد الأوروبي (القرار الإطاري JHA/2005/222)[8]	الاتحاد الأوروبي (المشروع التوجيهي 2010/073)[9]	الاتحاد الأوروبي (القرار الإطاري JHA/2001/413)[10]	الاتحاد الأوروبي (التوجيه EU/92/2011)[11]	الاتحاد الدولي للاتصالات CTU/CARICOM/(ITU) (نصوص[12]	الاتفاقية العربية لمكافحة جرائم المعلومات[13]	القانون النموذجي العربي بشأن مكافحة الجريمة السيبرانية[14]	منظمة شنغهاي للتعاون[15]	الأمم المتحدة (اتفاقية حقوق الطفل–البروتوكول الاختياري)[16]
المبادئ العامة للتعاون الدولي	المادة 14	المادة 41		المادة 5	المادة 23	المادة 1/38									المادة 5–3	المادة 10
تسليم مرتكبي الجريمة وفقا للصك		المادة 2/42			المادة 24	المادة 3/38				المادة 10			المادة 31			المادة 5
المساعدة القانونية المتبادلة العامة		المادة 43/أ 45		المادة 6	المواد 25 27	المادة 3/38	المادة 35			المادة 11			المواد 32 34			المادة 6
آليات المساعدة العاجلة		المادة 43/ب		المادة 2/6 1/7	المادة 3/25								المادة 3/32			
المساعدة/التحفظ على البيانات الحاسوبية		المادة 46			المادة 29								المادة 37			
المساعدة لجمع البيانات الحاسوبية والكشف عنها		المواد 47 48 51			المواد 30 31 34								المواد 39 41 42			
الوصول للبيانات الحاسوبية عبر الحدود الإقليمية		المادة 49/ب			المادة 32/ب								المادة 2/40			

تقديم المعلومات غير المرغوب فيها/تبادل المعلومات		المادة 44			المادة 26			المادة 11	المادة 14	المادة 12			المادة 33			
طلب السرية		المادة 45/ج		المادة 9	المادة 28								المادة 36		المادة 6	
التجريم المزدوج		المواد 42/أ 43/ب			المواد 1/24 3/25								المواد 5/32 3/37 4/37			
انشاء وحدة اتصال أو شبكة **7/24**		المادة 52			المادة 35			المادة 11	المادة 14				المادة 43			

مسؤولية والتزامات مقدمي الخدمة	الاتحاد الأفريقي[1]	السوق المشتركة لشرق أفريقيا والجنوب الأفريقي[2]	الكومنولث[3]	كومنولث اتحاد الدول المستقلة[4]	مجلس أوروبا (اتفاقية بودابست والبرتوكول الاختياري)[5]	مجلس أوروبا (اتفاقية لانزروت)[6]	الجماعة الاقتصادية لدول غرب أفريقيا[7]	الاتحاد الأوروبي (القرار الإطاري JHA/2005/222)[8]	الاتحاد الأوروبي (المشروع التوجيهي 2010/073)[9]	الاتحاد الأوروبي (القرار الإطاري JHA/2001/413)[10]	الاتحاد الأوروبي (التوجيه EU/92/2011)[11]	الاتحاد الدولي للاتصالات CTU/CARICOM/(ITU) (نصوص تشريعية نموذجية)[12]	الاتفاقية العربية لمكافحة جرائم المعلومات[13]	القانون النموذجي العربي بشأن مكافحة الجريمة السيبرانية[14]	منظمة شنغهاي للتعاون[15]	الأمم المتحدة (اتفاقية حقوق الطفل – البروتوكول الاختياري)[16]
التزامات المراقبة		المادة 17								المادة 15		المادة 28				
تقديم المعلومات طوعا		المادة 17/ب														
تسجيل الإخطارات		المادة 16														
مسؤولية مقدمي الوصول		المادة 12								المادة 12	المادة 29					
مسؤولية مقدمي التخزين المؤقت		المادة 13								المادة 13	المادة 31					
مسؤولية مقدمي الاستضافة		المادة 14								المادة 14	المادة 30					
مسؤولية مقدمي الروابط على الموقع/محركات البحث		المادة 15									المواد 32 33					

1 الاتحاد الأفريقي، 2012. مشروع اتفاقية بشأن إنشاء إطار قانوني للمساعدة في الأمن السيبراني في أفريقيا.

2 السوق المشتركة لشرق وجنوب أفريقيا (الكوميسا)، 2011. مشروع القانون النموذجي بشأن الأمن السيبراني.

3 الكومنولث 2002، (1) مشروع قانون الحاسوب والجرائم ذات الصلة بالحاسوب، (2) القانون النموذجي بشأن الأدلة الإلكترونية (مشار إليه بعلامة (*)).

4 كومنولث اتحاد الدول المستقلة، 2001. اتفاقية بشأن التعاون في مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية.

5 مجلس أوروبا، 2001. اتفاقية بشأن الجريمة السيبرانية والبرتوكول الإضافي للاتفاقية بشأن الجريمة السيبرانية، المعني بتجريم الأفعال ذات الطبيعة العنصرية أو كراهية الأجانب المرتكبة بواسطة النظم الحاسوبية.

6 مجلس أوروبا، 2007، اتفاقية حماية الأطفال ضد الاستغلال الجنسي والاعتداء الجنسي.

7 الجماعة الاقتصادية لدول غرب أفريقيا، 2009. مشروع توجيهي بشأن مكافحة الجريمة السيبرانية داخل دول غرب أفريقيا.

8 مجلس أوروبا، 2005. القرار الإطاري للمجلس 2005/222/JHA بشأن الهجمات ضد نظم المعلومات.

9 الاتحاد الأوروبي، 2010. المشروع النهائي التوجيهي للجنة التنفيذية (2010) 517 بالبرلمان الأوروبي ومجلس أوروبا بشأن الهجمات ضد نظم المعلومات وإلغاء القرار الإطاري للمجلس 2005/222/JHA.

10 الاتحاد الأوروبي، 2001. القرار الإطاري للمجلس الأوروبي 2001/413/JHA لمكافحة الاحتيال والتزوير ووسائط الدفع غير النقدية.

11 الاتحاد الأوروبي، 2011. التوجيه 2011/92/EU للبرلمان الأوروبي ومجلس أوروبا بشأن مكافحة الاعتداء الجنسي والاستغلال الجنسي للأطفال واستغلال الأطفال في المواد الإباحية، وإلغاء القرار الطاري للمجلس 2004/68/JHA.

12 الاتحاد الدولي للاتصالات/الجماعة الكاريبية/الاتحاد الكاريبي للاتصالات، 2010 (1) النصوص التشريعية النموذجية بشأن الجريمة السيبرانية/الجرائم الإلكترونية، (2) الأدلة الإلكتروني (مشار إليها بالعلامة (*)).

13 جامعة الدول العربية، 2010. الاتفاقية العربية بشأن مكافحة جرائم تقنية المعلومات.

14 جامعة الدول العربية، 2007. القانون العربي النموذجي لمكافحة الجرائم المتعلقة بنظم تكنولوجيا المعلومات.

15 منظمة شنغهاي للتعاون، 2010، اتفاقية التعاون في مجال أمن المعلومات الدولية.

[16] الأمم المتحدة، 2000. البروتوكول الاختياري الملحق باتفاقية حقوق الطفل بشأن بيع الأطفال وبغاء الأطفال واستغلال الأطفال في المواد الإباحية.

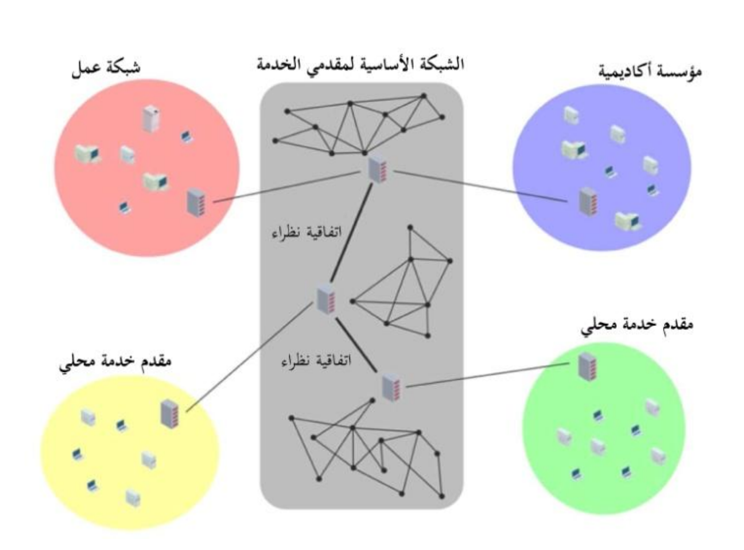
[17] الاتحاد الأوروبي، 2002. التوجيه 2002/58/EC الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن بمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية.

[18] الاتحاد الأوروبي، 2006. التوجيه 2006/24/EC الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الاحتفاظ بالبيانات التي تم إنشاؤها أو معالجتها فيما يتعلق بتوفير خدمات الاتصالات الإلكترونية المتاحة للجمهور أو شبكات الاتصالات العامة.

[19] الاتحاد الأوروبي، 2000. التوجيه 2000/31/EC الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الجوانب القانونية المحددة لخدمات مجتمع المعلومات في الأسواق الداخلية، ولاسيما التجارة الإلكترونية.

الملحق الرابع: الإنترنت

الإنترنت هو عبارة عن *مجموعة* من الشبكات التي تتصل فيما بينها – وأما كلمة "الإنترنت" فهي في حد ذاتها مجرد اختصار لكلمة "آلية ربط عدة شبكات صغيرة ببعض لتكوين شبكة ضخمة". تتكون هذه الشبكات بشكل أساسي من أجهزة حاسوب فردية، التي تتراوح بدءا من أجهزة الحاسوب الشخصية إلى أجهزة الحاسوب العملاقة التي تتصل مع بعضها بعضا من خلال البنية التحتية العالمية للكابلات المادية والروابط اللاسلكية.



وتعمل *أجهزة التوجيه* *(Routers)* على نقل البيانات من خلال هذه الشبكات، وتتراوح أشكالها ما بين أجهزة صغيرة منخفضة القدرة أو آلات قوية عالية القدرة تتعامل مع الآلاف من الاتصالات الفردية والكميات الكبيرة من الحركة. وتقوم أجهزة التوجيه بضم شبكات الحاسوب الفردية معا لتشكل شبكة الإنترنت ونقل المعلومات وتقديم التوجيهات الرقمية التي تسمح لأجهزة الحاسوب بالاتصال مع بعضها بعضا في أي مكان في العالم.

كيفية عمل الإنترنت

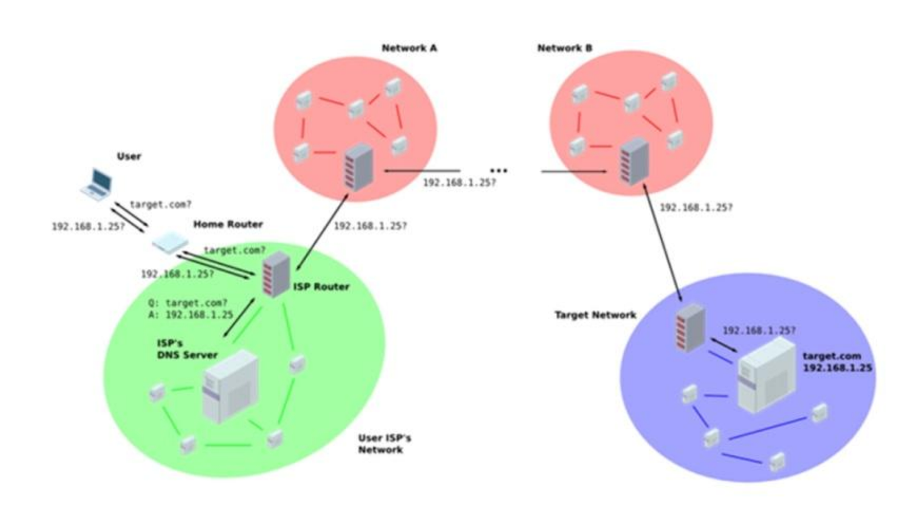
هناك أنماط عديدة من حركة الإنترنت. أشهر تلك الأنماط متصل بالشبكة العنكبوتية العالمية، والذي تم تطويره لأول مرة في المركز الأوروبي للأبحاث النووية (CERN) في نهاية عام 1980. تم تصميم شبكة الإنترنت في بداية الأمر كنظام وثائق يحتوي على روابط لوثائق أخرى – وهو مفهوم يعرف باسم "النص الفائق" (hypertext) الذي تم اقتراحه في وقت مبكر من العام 1930.[1]

من خلال النقر على الرابط في متصفح الإنترنت، تبدأ سلسلة من العمليات التي تؤدي إلى عرض صفحة ويب جديدة على الحاسوب. تتضح هذه العملية في الشكل المبين أدناه. تقوم الخطوة الأولى بترجمة الاسم الذي يمكن قراءته للخدمة، مثل www.target.com، إلى *عنوان* بروتوكول الإنترنت العددي (IP) الذي يمكن لأجهزة الحاسوب استخدامه لتحديد موقع أجهزة الحاسوب الأخرى على شبكة الإنترنت. يتم ذلك باستخدام خادم نظام أسماء النطاقات (DNS)، الذي يتم تشغيله عادة من قبل مزود خدمة الإنترنت (ISP) الخاص

[1] Ziewitz, M. and Brown, I. 2013. A prehistory of Internet governance. *In* Brown, I. *Research Handbook on Governance of the Internet.* Cheltenham: Edward Elgar.

بالمستخدم، والذي يكون موقعه عادة مقدّم لحاسوب المستخدم عند اتصالهم لأول مرة. يوجد هناك العديد من خوادم نظام أسماء النطاقات (DNS) البديلة المتاحة – ومن الأمثلة الشهيرة عليها على سبيل المثال تلك التي يتم تشغيلها من قبل أوبن دي إن إس (OpenDNS)، كذلك قبل جوجل (Google).[1]

بمجرد معرفة عنوان بروتوكول الإنترنت (IP) للحاسوب البعيد، يمكن إرسال المعلومات إليه. يمكن أن يتخذ ذلك شكل طلبات للبيانات، مثل صفحة ويب، والتي يتم بعد ذلك إرسالها إلى متصفح ويب المستخدم. وللقيام بذلك يتم تقسيم المعلومات إلى سلسلة من الحزم – كميات صغيرة من البيانات- التي تنتقل بشكل مستقل عبر الإنترنت قبل أن يتم تجميعها عن بعد على الحاسوب البعيد. تحتوي كل حزمة على عنوان بروتوكول الإنترنت للحاسوب عن بعد، والمعلومات المتعلقة بنمط البيانات المدرجة في الحزمة، وعينة البيانات نفسها.



لا تشمل الحزم عموما المعلومات خلال الطريق إلى وجهتها. بدلا من ذلك، فهي اشبه منها بالنظام البريدي، حيث تعطي الوجهة فقط. تحدد أجهزة التوجيه المقابلة للحزمة أنجع وسيلةٍ للوصول إلى الوجهة. ومن خلال القيام بذلك يمكن للإنترنت الاستجابة بسرعة ومرونة في حالة تلف جزء من الشبكة أو حملت فوق طاقتها، من خلال اختيار مسارات بديلة للبيانات.

آليات الاتصال

تستند الإنترنت إلى مجموعة من المعايير التقنية لنقل وتوجيه البيانات. يحدد *بروتوكول الإنترنت* كيفية تقسيم البيانات إلى قطع للانتقال، وكذلك كيفية تحديد عناوين المصدر والمقصد. يعد الإصدار الرابع هو الأكثر شيوعا (النسخة الرابعة من بروتوكولات الإنترنت IPv4)، على الرغم من أن هناك إندفاع قوي نحو إصدار أحدث وهو النسخة السادسة من بروتوكولات الإنترنت. يتم "وضع" طبقات من البروتوكولات الإضافية على رأس بروتوكول الإنترنت الأساسي من أجل بناء خدمات مثل الشبكة. تعد الحزمة الأكثر شيوعا من هذه البرتوكولات

[1] أنظر: http://www.opendns.com and https://developers.google.com/speed/public-dns/

هي بروتوكول التحكم في الإرسال (TCP) الذي يوفر آلية تسليم موثوق به ويمنع إرسال الكثير من البيانات في وقت واحد. ومن تلك البرتوكولات أيضا برتوكول آخر يسمى بروتوكول بيانات المستخدم (UDP) الذي لا يقدّم أي ضمانات للتسليم، ولكن يسمح بنقل يتميز بالكفاءة العالية والمرونة للاتصالات الآنية (real-time) مثل الصوت.

لكل حاسوب على شبكة الإنترنت عنوان فريد مكتوب في شكل "الرباعي المنقط" مثل 192.168.1.1. تستخدم أجهزة التوجيه عناوين بروتوكولات الإنترنت هذه لتوجيه كل حزمة إلى وجهتها. يقوم بروتوكول التحكم في الإرسال (TCP) وبروتوكول بيانات المستخدم (UDP) بإضافة "أرقام المنافذ" التي تحدد الخدمة التي يتم توجيه الحزمة إليها وهي:

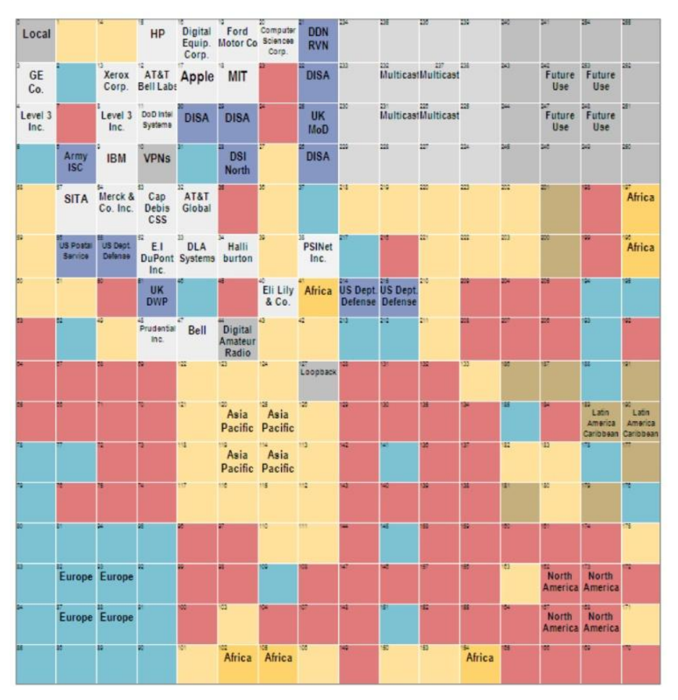
الخدمة	النقل	رقم المنفذ
بروتوكول نقل البريد البسيط SMTP (البريد الإلكتروني)	بروتوكول التحكم في الإرسال (TCP)	25
الويب (بروتوكول نقل النصوص المترابطة HTTP)	بروتوكول التحكم في الإرسال (TCP)	80
ويب آمن (بروتوكولات نقل النصوص المترابطة HTTPs)	بروتوكول التحكم في الإرسال (TCP)	443
نظام أسماء النطاقات (DNS)	بروتوكول بيانات المستخدم (UDP)	53
القشرة الآمنة SSH (القشرة الآمنة عن بعد)	بروتوكول التحكم في الإرسال (TCP)	22

يشرف على توزيع المجموعات الثلاث من المعرفات الفريدة للإنترنت – أسماء النطاقات، وعناوين بروتوكولات الإنترنت والنظام الذاتي (AS)، وأرقام منفذ البروتوكول والوسيط – هيئة نفع عام غير ربحية في الولايات المتحدة الأمريكية: آيكان؛ (هيئة الإنترنت للأسماء والأرقام المخصصة ICANN).[1] بالإضافة إلى ذلك، تقوم هيئة آيكان بتنسيق تشغيل وتطوير نظام خادم رئيسي لأسماء النطاقات، وتنسيق وضع سياسة تتعلق بهذه الوظائف الفنية.[2] يتم تفويض مهام توزيع وتسجيل موارد الإنترنت إلى خمس تسجيلات إنترنت إقليمية التي توزع "كتل" عناوين بروتوكولات الإنترنت إلى منظمات مثل مقدمي خدمة الإنترنت والمؤسسات الأكاديمية.

[1] عقد تأسيس هيئة الإنترنت للأرقام والأسماء المخصصة المتاحة في: http://www.icann.org/en/about/governance/articles

[2] هيئة الإنترنت للأرقام والأسماء المخصصة 2012. *Bylaws for Internet Corporation for Assigned Names and Numbers.*

هناك عدد محدود من عناوين النسخة الرابعة من بروتوكولات الإنترنت المتاحة. عدد عناوين النسخة الرابعة من بروتوكولات الإنترنت "32-bit" – الأرقام التي يمكن التعبير عنها ثنائيا باستخدام 32 رقم – تسمح لعدد 2^{32}، أو ما يقرب من 4.3 بليون عنوان. وبما أن الإنترنت قد نما فوق كل التوقعات فإن هذه الأرقام تنفذ بسرعة دون ترك أيّ مسافة لإضافة أجهزة جديدة يمكن إضافتها. واستجابة لذلك، يجري حاليا بذل جهد كبير لتحديث شبكة الإنترنت لنسخة جديدة من بروتوكول الإنترنت، النسخة السادسة من بروتوكول الإنترنت (IPv6). توسع النسخة السادسة من بروتوكول الإنترنت العدد المتاح من العناوين التي تستخدم أرقام 128 بت، منشئة 2^{128} عنوانا – مكتوبة في نظام العد العشري، وهذا العدد طوله 39. من المؤمل أن يكون هذا كافيا في المستقبل المنظور. يوضح الشكل الموجود أعلاه مساحة عنوان النسخة الرابعة من بروتوكول الإنترنت الحالية الكلية المتاحة والمخصصة.[1] يتم تخصيص كتل كبيرة من عناوين النسخة الرابعة من بروتوكول الإنترنت المتاحة للسجلات الإقليمية. ولأسباب تاريخية تم تخصيص بعض الكتل ذات المستوى العالي، مثل الكتلة 18.x.x.x للقطاع الخاص الفردي، المنظمات الأكاديمية أو الحكومية.



نظام اسم النطاق (DNS)

ومن أجل زيادة إمكانية وصول المستخدمين، فإن العناوين الموجودة على الإنترنت مكتوبة أيضا بصفتها أسماء نطاق من خلال استخدام نظام اسم النطاق. فضلا عن تخصيص عنوان بروتوكول الإنترنت، تقوم هيئة آيكان بإدارة نظام اسم النطاق من خلال سلطة مفوضة لتسجيل أسماء النطاق. تتكون عملية التسجيلات هذه من قواعد بيانات لجميع أسماء النطاقات المسجلة ضمن *النطاق العام من المرتبة العليا*، مثل (.com, .net, .int, .mil, .gov) ونطاق عنوان البلد مثل (.de) وتدل على ألمانيا، (.cn) وتدل على دولة الصين. وتكون التسجيلات مسؤولة عن الحفاظ على البيانات الموثقة الخاصة بمكان إمكانية الحصول على نطاق.

عند عملية تسجيل نطاق جديد، فعادة ما يتم التعامل معها من خلال أحد المسجلات العديدة. وتتحقق هذه الشركة من عدم وجود النطاق الجديد بالفعل، ومن ثم تخطر السجل المركزي بشأن طلب نطاق

---
[1] سلطة تخصيص أسماء الإنترنت (آيانا) 2012 .*IANA IPv4 Address Space Registry*

جديد، جنبا إلى جنب مع معلومات بشأن مكان الحصول على تفاصيل موثقة تتعلق بالنطاق. ثم يتم ترحيل هذه المعلومات، على مدى ما يقرب من 24 ساعة، إلى خوادم نظام اسم النطاق الرئيسية في جميع أنحاء العالم.

تحت كل نطاق من النطاقات ذات المرتبة العليا توجد أسماء منظمات متشابهة قد قامت بتسجيل الاسم. شركة جوجل على سبيل المثال، قامت بتسجيل اسم "جوجل" ضمن نطاق (com.) ذو المرتبة العليا، لإيجاد نطاق google.com. ربما تقوم أجهزة الحاسوب بإعطاء أسماء فردية ضمن النطاق الخاص بها. إن الاسم 'www' هو بمثابة اسم معياري لأجهزة الحاسوب التي تقوم بتشغيل خادم الويب، وكذلك فإنه من المعتاد رؤيته في بداية عنوان أي موقع مثل www.google.com[1] . وعلى النحو نفسه فإن mail.google.com تشير إلى أجهزة الحاسوب التي تقدم خدمات GMail التابعة لجوجل. وتنقسم بعض النطاقات ذات المرتبة العليا إلى العديد من المجموعات مثل "co." لأغراض الأعمال التجارية أو ac. للجامعات، وعلى سبيل المثال ما هو قائم في المملكة المتحدة. وهذا يعني أن ظهور جوجل على الإنترنت في المملكة المتحدة يسجل على www.google.co.uk.

سوف يسمح برنامج *النطاق العام من المرتبة العليا* الخاص بهيئة آيكان لإيجاد نطاقات ذات مرتبة عليا، الأمر الذي يسمح لتسجيل أسماء مثل baby. و book. يرتفع مستوى تعقيد وتكلفة تسجيل نطاقات عامة ذات مرتبة عليا، ولكن البرنامج سيوسع من أرقام البدائل المحتملة لأسماء النطاق توسيعا هائلا.

الاتصال المحدود

تم اتصال العديد من أنحاء جنوب وشرق أفريقيا بخدمات الإنترنت السريع، من خلال مد كابل بحري للمرة الأولى في أواخر عام 2009. وبحلول عام 2012، أصبحت قارة أفريقيا لا تشكل سوى 6 في المائة من حجم الاتصال بشبكة الإنترنت العالمية.

وقد فاق عدد الاتصال بالإنترنت القائم على الهواتف النقالة عدد الاتصال القائم على الخطوط الأرضية منذ عام 2008. وفي كثير من أنحاء قارة أفريقيا، بالرغم من التحسينات التي لحقت بالبنية التحتية المتوفرة، تظل الهواتف النقالة بعيدة إلى حد ما عن طريقة الوصول إلى الخدمات القائمة على الإنترنت الأكثر شيوعا. وأدى هذا إلى مجموعة من الخدمات التي ترمي لصالح مستخدمي الهواتف النقالة، بدءا من العملات الإلكترونية التي تستند على أرصدة الهاتف النقال، ووصولا إلى نتائج البحث التي تنقل عبر خدمة الرسائل النصية القصيرة SMS.

الخدمات المشتركة

واحدة من أكثر التطبيقات شيوعا على الإنترنت في بدايته هي البريد الإلكتروني، وتبقى بمثابة خدمة رئيسية — أصبح عنوان البريد الإلكتروني يحظى بنفس القدر من الأهمية الذي تحظى به أرقام التليفون أو العنوان الفعلي لكثير من المعاملات الحديثة.

فضلا عن البريد الإلكتروني، فقد كان الويب بمثابة القوة الدافعة لعالم الإنترنت، والذي تزامن مع الازدهار الذي شهده عدد المستخدمين المنزليين الذين يتصلون بالإنترنت في التسعينات. ومنذ

[1] في واقع الأمر تقوم شركة جوجل بتشغيل المواقع الإلكترونية الخاصة بها على العديد من أجهزة الحاسوب المختلفة. في حقيقة الأمر، فإن اسم 'www' هو اسم مستعار يشير إلى العديد من أجهزة الحاسوب المختلفة على النحو المطلوب.

ذلك الحين، فقد ساعدت أدوات ما تسمى 'Web 2.0' على نمو حجم المحتوى المقدم من طرف المستخدمين. وتسمح هذه المواقع الإلكترونية للمستخدمين بمشاركة حياتهم واهتماماتهم مع أصدقائهم، فضلا عن رفع صور وفيديوهات، بالإضافة إلى إنشاء مجلات أو مدونات، علاوة عن استضافته للعديد من الأنشطة الأخرى، كما أن خدمة نقل الصوت عبر بروتوكول الإنترنت (VoIP) تحتل الآن المرتبة الثالثة من حيث الاستخدام على نطاق واسع. يسح هذا بإجراء المكالمات الهاتفية، والأكثر من ذلك، مكالمات الفيديو والمكالمات الجماعية بتكلفة منخفضة وبسهولة على الإنترنت. من التقنيات الرئيسة النهائية شبكات الند للند (P2P) التي توصل حواسيب المستخدمين مباشرة فيما بينها لغرض مشاركة الملفات أو البيانات، وذلك على نقيض الخدمات التقليدية حيث تكون الموصولية من خلال *خادم* مركزي. من أحدث شبكات الند للند الشائعة نابستر وجنوتيلا التي تركز في الأساس على مشاركة ملفات الموسيقى. وفي الآونة الأخيرة، سمح نظام بت تورنت بمشاركة الملفات الكبيرة بسرعة وكفاءة، مثل: تطبيقات البرمجيات وملفات الفيديو.

ويعمل نظام بت تورنت من خلال السماح للمستخدمين بتحميل أجزاء من البيانات ورفعها. ولتوزيع أي ملف كبير الحجم، مثل: ملفات الفيديو، يقسمه بت تورنت إلى أجزاء صغيرة يحملها المستخدمون الذين يتيحون الأجزاء التي قاموا بتحميلها بالفعل مع الآخرين من أجل تحميلها . وينتج عن ذلك زيادة عدد المستخدمين الذين يحملون الملف وزيادة عدد المستخدمين المشاركين لأجزاء الملف، مما يزيد سرعة التحميل للمستخدمين الآخرين. وينعكس نجاح هذا النهج في أن بت تورنت يمثل ما يتراوح ما بين 10 و15 في المائة من إجمالي استخدام الإنترنت في أوروبا أمريكا الشمالية في النصف الثاني من عام 2012.[1]

الحوكمة

منذ أيامها الأولى، كان لعدد من المؤسسات تأثير على تطوير الإنترنت وتشغيله. بعض منها جهات حكومية تقليدية، والبعض الآخر شركات، ولا يزال البعض الآخر مجموعات من المتطوعين.[2]

جهة وضع المعايير الأساسية هي فريق العمل المعنية بهندسة الإنترنت. حيث أنها تتألف من متطوعين من جميع أنحاء العالم، ويعمل فريق العمل المعني بهندسة الإنترنت على تطوير المعايير الجديدة وتبنيها من أجل تعزيز تقنيات الإنترنت بالإضافة إلى التنسيق مع جهات المعايير الأخرى. وأشهر النتائج الصادرة عن فريق العمل المعنية بهندسة الإنترنت هي طلب التعليقات. حيث أنها تصف بروتوكولات الإنترنت الجديدة بكل صراحة حتى يستطيع أي شخص بناء تقنيات متوافقة.

[1] ساندفين. 2012. التقرير العالمي لظاهرة الإنترنت، *2H 2012*.

[2] Ziewitz, M. and Brown, I. 2013. A prehistory of Internet governance. *In* Brown, I.*Research Handbook on Governance of the Internet*. Cheltenham: Edward Elgar.

كما تدير شركة الإنترنت للأسماء والأرقام المخصصة (آيكان) عناوين بروتوكول الإنترنت وأسماء المجال. آيكان هي شركة خاصة لا تهدف إلى الربح ومسجلة في أمريكا الشمالية. ويتضمن الهيكل التنظيمي لشركة آيكان ثلاثة اجتماعات سنوية للجنة الاستشارات الحكومية والتي توفر منتدى لتلقي المشورة والتمثيل من الحكومات الوطنية.

ويضع الاتحاد الدولي للاتصالات معايير للاتصالات الهاتفية والتلغرافية بالإضافة إلى الطيف الراديوي. وتعتبر لوائح الاتصالات الدولية مكملة لاتفاقية الاتصالات الدولية وتصحبها رؤية لتأسيس المبادئ العامة التي تتعلق بإمداد وتشغيل الجوانب المختلفة من الاتصالات العالمية بما فيها التدفق المروري وجودة الخدمة. وتمت صياغة لوائح الاتصالات الدولية قبل ظهور الإنترنت باعتباره نقطة انطلاق للاتصالات الدولية المهيمنة، وعلى هذا النحو فإنه لا يجعل إشارة خاصة للإنترنت ذاته.

توجيه الانترنت

عندما ترسل أجهزة الحاسوب معلومات عبر الإنترنت، فإنها تسافر عبر العديد من الشبكات قبل الوصول إلى وجهتها. ولتحديد أفضل توجيه تعلن الشبكات عن قدرتها في التعامل مع بعض التوجيهات باستخدام بروتوكول يسمى بروتوكول البوابة الحدودية.

بروتوكول البوابة الحدودية هو أحد البروتوكولات الأساسية على الإنترنت ولكنه يتمتع بخصائص أمنية قليلة محددة في البروتوكول وأخطاء تكوين يمكن أن يكون لها عواقب وخيمة. على سبيل المثال في أوائل عام 2010 بدأت جهات مقدمي خدمات الإنترنت الصغيرة في آسيا الشرقية للإعلان عن ما يقرب من 35,000 توجيه بين الشبكات بدلا من الرقم المعتاد 40. وكانت النتيجة أن تقريبا 10 في المائة من الشبكات العالمية أفيد بأنها قد تم توجيهها عن طريق الخطأ لمدة حوالي عشرين دقيقة.

التاريخ

من الممكن أن ترجع جذور نشأة الإنترنت إلى مشروع بحث أجرته وكالة مشاريع البحوث المتقدمة (والتي عرفت باسم ARPA وفيما بعد باسم DARPA) التابعة لوزارة الدفاع الأمريكية، وقد بدأت تلك الوكالة في عام 1969 والتي تهدف للسماح بالوصول عن بعد إلى موارد الحوسبة النادرة آنذاك التي تستضيفها الشركات والمؤسسات الأكاديمية.

تختلف الشبكة التي نشأت عن هذا المشروع، والمعروفة باسم شبكة وكالة مشاريع البحوث المتقدمة (أربانت)، اختلافا جذريا عن شبكات الاتصالات السابقة في توظيف المفهوم الذي تم تطويره حديثا ألا وهو تبادل حزم البيانات عبر شبكة الإنترنت بدلا من الطريقة التقليدية تبديل الدارة مما أدى إلى المزيد من القوة والفاعلية في خطوط الاتصال غير الموثوق بها المتاحة في ذلك الوقت.

نمت أربانت بسرعة مثلما هو الحال مع شبكات مماثلة مختلفة في كل من الولايات المتحدة الأمريكية وأوروبا. ومع تزايد عدد الشبكات، قامت وكالة مشاريع البحوث المتقدمة بتمويل الأبحاث التي يجريها فينت سيرف وآخرون لإيجاد وسيلة لهذه الشبكات للتواصل مع بعضها البعض. وكانت نتيجة هذا العمل المواصفات الأولى لبروتوكول التحكم بالإرسال في عام 1973 الذي وفر وسيلة مشتركة لربط الشبكات المختلفة معا وتضمنت أول استخدام لمصطلح "الإنترنت". كما ظلت التقنيات التي تم تطويرها لهذا العمل في صميم الإنترنت المتعارف عليه حاليا.

وفي عام 1989 قام تيم بيرنرز لي، الذي يعمل لدى المركز الأوروبي للأبحاث النووية (CERN)، بتطوير شبكة الإنترنت العالمية والتي سمحت للوثائق أو الصفحات أن تتصل بالوثائق الأخرى المخزنة عبر الشبكة. وتم إعداد البرنامج ليكون متاحا بالمجان وأصبح مشهورا للغاية خلال أوائل التسعينيات.

وتم تخفيف القيود على النشاط التجاري على الإنترنت في عام 1994، وتسبب هذا بالإضافة إلى زيادة شعبية الإنترنت بزيادة الاستخدام التجاري والشخصي للإنترنت خلال التسعينيات. وقام مقدمو خدمات الإنترنت التجارية بتوصيل المستخدمين بالإنترنت وبمجموعة آخذة في التوسع من أدوات وخدمات المعلومات. وشهد منتصف التسعينيات ظهور أول الشركات التي تعتمد على الإنترنت اعتمادا كبيرا وحقيقيا، بشكل رئيسي محركات البحث الأولى، التي ساعدت في فهم مجموعة كبيرة من المعلومات المتاحة حاليا. وكان ياهوو الذي تأسس في عام 1994 محرك البحث الرئيسي وتبعه جوجل في عام 1998.

ومنذ ذلك الحين، أفسحت المواقع الثابتة والبسيطة الطريق للمواقع التفاعلية التي تسمح للمستخدمين بتصميم المحتوى ومشاركته مما أدى إلى ظهور الشبكات الاجتماعية. وزادت سرعة الاتصال مما سمح ببث الفيديوهات والموسيقى لأجهزة الحاسوب المنزلية.

الإعلانات المستهدفة

يعدّ الإعلان الصورة السائدة للأعمال على الويب، حيث تبيع المواقع الإلكترونية، مثل: جوجل وفيسبوك وياهوو! مساحة إعلانية للشركات من أجل تقديم الإعلانات إلى ملايين المستخدمين الذين يطلعون عليها يوميا.

تتاح خدمات، مثل: فيسبوك وجوجل، للمستخدمين مجانا. والأكثر من ذلك، هذه المواقع تتبع نشاط المستخدمين، وتحلل البيانات (أو تنقب عنها) من أجل إنشاء الملفات التي تستخدم فيما بعد لتقديم الإعلانات "المستهدفة" الموجهة بحسب اهتمامات المستخدمين.

وقد أدى نجاح هذا النوع من الخدمات المجانية بمساعدة الإعلانات المستهدفة إلى تحقيق جوجل إيرادات سنوية بقيمة 50 مليار دولار أمريكي، كما أصبحت قيمة شركة فيسبوك 104 مليار دولار أمريكي عندما طرحت أسهمها لأول مرة في البورصة في منتصف عام 2012.

الحوسبة السحابية

مع تطور الإنترنت، تظهر نُهُج جديدة في الحوسبة، وقد يكون أبرزها هي *الحوسبة السحابية*.

فبدلا من تخزين المعلومات على حواسيب المنزل أو العمل، أو شراء البرامجيات وتحديثها، تسمح السحابة للمستخدمين بتحميل بياناتهم على خوادم الإنترنت وتشغيل برامجهم عن بعد. تسمح طريقة الاستعانة بمصادر خارجية هذه لعدد كبير من *مزودي الخدمات السحابية* بالاحتفاظ بمراكز مخصصة ذات نطاق واسع من البيانات باعتبارها الوجود المادي للحوسبة السحابية. وتمثل مراكز البيانات هذه مواقع مخصصة يمكن إدارة بنوك الحواسيب الكبيرة داخلها مركزيا وتوصيلها بالإنترنت فائق السرعة في ظل متطلبات طاقة محددة.

تقدم الحوسبة السحابية مميزات من حيث التكلفة والكفاءة، ولكن أيضا تصحبها بعض المخاطر: تكون البيانات الخاصة أو السرية المخزنة في السحابة جاذبة للمتسللين، في حال انهيار اتصال الشركة بالإنترنت لا يمكن الوصول إلى البيانات أو إجراء الأعمال، في حال انقطاع خدمة الحوسبة السحابية أو هجوم المتسللين عليها تتأثر الأعمال والأشخاص الذين يستخدمونها.

الملحق الخامس: النهج المستخدم

النهج الذي تبنته مجموعة الخبراء

تبنت المجموعة المفتوحة لخبراء الحكومات الدولية بشأن الجريمة السيبرانية في دورتها الأولى، المعقودة من 17 حتى 21 كانون الأول/يناير 2011، "نهج الدراسة":[1]

1. من أجل تحقيق ولاية مجموعة الخبراء بشأن الدراسة، وضع الهيكل المذكور أدناه لتسهيل إجراء الدراسة، والذي سوف ينفذ تحت إشراف مجموعة الخبراء.

2. يحق لكل بلد أن تقدم ما لديها من آراء، وينبغي أن تنعكس في الدراسة.

3. سوف يتولى مكتب الأمم المتحدة المعني بالمخدرات والجريمة مهمة تطوير الدراسة، بما في ذلك وضع استبيان، وتجميع البيانات وتحليلها، ووضع مسودة مكتوبة للدراسة. ولتحقيق هذه المهمة، سوف يعتمد مكتب الأمم المتحدة المعني بالمخدرات والجريمة على خبرته الداخلية وإمكاناته على مختلف الفروع الموضوعية لمكتب الأمم المتحدة المعني بالمخدرات والجريمة (شعبة شؤون المعاهدات، فرع السياسات والبحوث). ولهذا الغرض، ينبغي إتاحة موارد خارج الموازنة بما يكفي لتمكين مكتب الأمم المتحدة المعني بالمخدرات والجريمة من أداء هذه المهام بكفاءة. ولمساعدة الأمانة على ضمان تقديم ما يكفي من الخبرة والأنظمة والاحتياجات التكنولوجية الأساسية؛ سوف تقدم كل مجموعة إقليمية للأمانة أسماء خبراء الحكومات (بما لا يزيد عن ستة)، ومعلومات الاتصال بهم، ومجال خبرتهم. وسوف تتشاور الأمانة مع هؤلاء الخبراء باعتبارهم مصدرا على أساس مخصص، بحسب الاقتضاء.

4. سوف تقدم الأمانة بانتظام مذكرة موجزة والمشورة للمكتب بشأن مجموعة الخبراء عن عملهم، وتعمم محاضر المشاورات على الدول الأعضاء. ليس الغرض من وضع قائمة بالخبراء هو عقد مجموعة مغلقة للخبراء أو إنشاء جهات فرعية من مجموعة الخبراء.

5. بالنسبة لتجميع المعلومات، سوف يعد مكتب الأمم المتحدة المعني بالمخدرات والجريمة استبيان لزيادة توزيعه على الدول الأعضاء والمنظمات الحكومية الدولية ومؤسسات القطاع الخاص (أنظر الجدول الزمني الإرشادي أدناه) الذي سوف يتكون من صك دراسة استقصائية وحيد وفقا للأطر المنصوص عليها في ورقة المفاهيم/العمل الخاصة بالاجتماع الأول لمجموعة الخبراء، وتعديلاتها، وبناء على مقترحات الاجتماع الأول لمجموعة الخبراء، على النحو الوارد في تقريرها.

[1] E/CN.15/2011/19

6. في المقام الثاني، بحسب الحاجة، سوف تتشاور الأمانة، مع أخذ الحاجة لتوازن العروض التقديمية من مختلف الأقاليم في الاعتبار، مع ممثلي القطاع الخاص، بمن فيهم ممثلو مزودي خدمات الإنترنت، مستخدمو الخدمات، غيرهم من الجهات الفاعلة المعنية الأخرى، وممثلو الأوساط الأكاديمية، من البلدان النامية والمتطورة، وممثلو المنظمات الحكومية الدولية المعنية.

الإجراءات المتخذة

اتبع هذا النهج من خلال الإجراءات الواردة أدناه:

17 حتى 21 كانون الثاني/يناير 2011	تبني "مجموعة مواضيع للنظر فيها في دراسة شاملة عن أثر الجريمة السيبرانية والاستجابة لها" و"نهج الدراسة والجدول الزمني الإرشادي" خلال الدورة الأولى للمجموعة المفتوحة لخبراء الحكومات الدولية بشأن الجريمة السيبرانية.
14 أيلول/سبتمبر 2011	قرار المكتب بمراجعة الجدول الزمني الإرشادي نتيجة لإتاحة الأموال تدريجيا للدراسة، وتعميم مشروع الاستبيان لا تعده الأمانة بالإنجليزية إلا للدول الأعضاء للتعليق عليه بحلول 31 تشرين الأول/أكتوبر 2011.
23 أيلول/سبتمبر 2011	إرسال مشروع الاستبيان للدول الأعضاء للتعليق عليه بموجب مذكرة شفوية CU 2011/168.
10 تشرين الأول/أكتوبر حتى 16 تشرين الثاني/نوفمبر 2011	استلام التعليقات المكتوبة عن الاستبيان من 18 دولة عضو تسجلها الأمانة إلى أقصى حد ممكن.
19 كانون الثاني/يناير 2012	إنهاء الاستبيان بمعرفة المكتب.
29 شباط/فبراير 2012	إرسال الاستبيان باللغات الستة الرسمية لجميع الدول الأعضاء بموجب مذكرة شفوية CU 2012/19 لاستيفائه بحلول 31 أيار/مايو 2012. ودعوة الدول الأعضاء لترشيح بعض منظمات القطاع الخاص أو المؤسسات الأكاديمية لاستلام الاستبيان بخصوص الدراسة. إرسال دعوات لمنظمات القطاع الخاص أو المؤسسات الأكاديمية والمنظمات الحكومية الدولية لاستيفاء الاستبيان بخصوص الدراسة الذي أُرسل.
15-19 نيسان/أبريل 2012	عقد حلقة عمل إقليمية لدعم الدراسة في نيروبي، كينيا بحضور 10 بلدان من أفريقيا ومنظمة حكومية دولية واحدة.
24-27 نيسان/أبريل 2012	عقد حلقة عمل إقليمية لدعم الدراسة في بيروت، لبنان بحضور 12 بلدا من غرب آسيا وشمال أفريقيا ومنظمتين حكومتين دوليتين.
5-10 أيار/مايو 2012	عقد حلقة عمل إقليمية لدعم الدراسة في بانكوك، تايلاند بحضور 11 بلدا من آسيا ومنظمة حكومية دولية واحدة.
11 أيار/مايو 2012	إرسال مذكرة شفوية CU 2012/102 بشأن الاستبيان بخصوص الدراسة

	لجميع الدول الأعضاء.
6 حزيران/يونيو 2012	إرسال مذكرة شفوية CU 2012/117 بشأن الاستبيان بخصوص الدراسة لجميع الدول الأعضاء. مد آخر موعد لاستيفاء الاستبيان حتى 30 حزيران/يونيو 2012.
13 أيلول/سبتمبر 2012	إرسال تقرير الأمانة إلى المكتب الموسع بشأن حالة الإجابات على الاستبيان، وتداول المكتب الموسع بشأن الخطوات التالية.
1 تشرين الأول/أكتوبر 2012	العرض المسبق للمعلومات عن التشريع ذي الصلة لتستخدمه الأمانة في التحليل، وإرسال المشروع إلى الدول الأعضاء بموجب مذكرة شفوية CU 2012/176، مع الدعوة لتقديم التعليقات والتصحيحات بحلول 9 نوفمبر 2012.
24 تشرين الأول/أكتوبر 2012	بعد اجتماع المكتب الموسع المؤرخ 13 أيلول/سبتمبر 2012، إصدار قرار رئيس المجموعة المفتوحة لخبراء الحكومات الدولية بشأن الجريمة السيبرانية خلال الأسبوع الذي يبدأ في 25 شباط/فبراير 2013.
24 تشرين الأول/أكتوبر حتى 30 كانون الثاني/يناير 2013	استلام التعليقات المكتوبة بشأن التشريع من 16 دولة عضو.
9 تشرين الثاني/نوفمبر 2012	إرسال النتائج المبدئية للدراسة إلى الخبراء الذين رشحتهم المجموعات الإقليمية.
6 كانون الأول/ديسمبر حتى 14 كانون الثاني/يناير 2013	استلام التعليقات المكتوبة بشأن النتائج المبدئية للدراسة إلى الخبراء الذين رشحتهم المجموعات الإقليمية.
30 كانون الثاني/يناير 2013	إرسال الملخص التنفيذي للدراسة الشاملة بشأن الجريمة السيبرانية إلى المشاركين المسجلين في الدورة الثانية للمجموعة المفتوحة لخبراء الحكومات الدولية بشأن الجريمة السيبرانية.
8 شباط/فبراير 2013	إرسال المشروع الكامل للدراسة الشاملة بشأن الجريمة السيبرانية إلى المشاركين المسجلين في الدورة الثانية للمجموعة المفتوحة لخبراء الحكومات الدولية بشأن الجريمة السيبرانية.
25 حتى 28 شباط/فبراير 2013	عقد الدورة الثانية للمجموعة المفتوحة لخبراء الحكومات الدولية بشأن الجريمة السيبرانية.

المعلومات المجمعة

جرى استلام إجابات البلدان الستة عشر على الاستبيان من الدول الأعضاء، وفقا للتوزيع الجغرافي التالي:

أفريقيا	شرق أفريقا	2
	شمال أفريقا	4
	جنوبي أفريقا	3
	غرب أفريقا	2
	الإجمالي	11
الأمريكتين	منطقة البحر الكاريبي	2
	أمريكا الوسطى	1
	أمريكا الشمالية	2
	أمريكا الجنوبية	8
	الإجمالي	13
آسيا	شرق آسيا	3
	جنوب شرق آسيا	4
	جنوب آسيا	4
	غرب آسيا	8
	الإجمالي	19
أوروبا	أوروبا الشرقية	8
	أوروبا الشمالية	6
	أوروبا الجنوبية	4
	أوروبا الغربية	6
	الإجمالي	24
أوقيانوسيا	أوقيانوسيا	2
	الإجمالي	2

دعت الأمانة أكثر من 1500 منظمة قطاع خاص، و380 منظمة أكاديمية، و80 منظمة حكومية دولية مباشرة، وفقا لنهج الدراسة، للمساهمة بالمعلومات من أجل الدراسة. تَحدد التوزيع الجغرافي المنصف لمنظمات القطاع الخاص من خلال الاتفاق العالمي للأمم المتحدة، الاتحاد الدولي للاتصالات، وعضويات الاتحادات الصناعية. كما تحددت المنظمات الأكاديمية من خلال قائمة بأفضل 500 جامعة. كما أجابت أربعون منظمة قطاع خاص، و16 منظمة أكاديمية، و11 منظمة حكومية دولية على الاستبيان بخصوص الدراسة أو استكملت مقابلة هاتفية بناء على الاستبيان الخاص بالدراسة:

منظمات القطاع الخاص	المنظمات الأكاديمية
Accenture	B-Ccentre
Aconite Internet Solutions Ltd.	جامعة بكين للمعلمين
Admiral Insurance Company	جامعة براون
Allen & Overy LLP	جامعة إبرهارد كارل في توبنغن
Betterley Risk Consultants, Inc.	النقابة الدولية لمحامي تكنولوجيا المعلومات
Casdisa de Promociones, S.A.	جامعة مازاريك
Cisco Systems, Inc.	المعهد الوطني لتقنية المعلومات والاتصالات
Cooperativa La Cruz Azul S.C.L.	كلية الشرطة النرويجية
Danfoss A/S	المعهد الملكي للتكنولوجيا في ملبورن
Digicel Group Ltd.	جامعة أديليد
Ernst & Young Global Limited	جامعة درم
Estudio de Informática Forense	جامعة إرلنغن نورنبيرغ
FIRST.org, Inc.	جامعة لوزان
Gloria Group	جامعة فريجي في بروكسل
Hewlett-Packard Company	جامعة واسيدا/كلية الحقوق
Hogan Lovells	جامعة شيان جياو تونغ
Huawei Technologies Co., Ltd.	**المنظمات الحكومية الدولية**
I2 Integrity International	مجلس أوروبا
InfoCom Research, Inc.	الاتحاد الأوروبي
Intyernational Cyber Security Protection Alliance	منظمة الأغذية والزراعة
Internet Security Aliance	الصندوق الدولي للتنمية الزراعية
ID Experts Corp.	الإنتربول
Juniper Networks, Inc.	منظمة الأمن والتعاون في أوروبا
KPMG International Cooperative	مؤتمر الأمم المتحدة للتجارة والتنمية (الأونكتاد)
Logica Pvt Ltd	برنامج الأمم المتحدة الإنمائي
McKinsey & Company, Inc.	مفوضية الأمم المتحدة لشؤون اللاجئين
Mitsubishi UFJ Financial Group, Inc.	معهد الأمم المتحدة الإقليمي لبحوث الجريمة والعدالة

هيئة الأمم المتحدة للمساواة بين الجنسين وتمكين المرأة	Nippon Telegraph and Telephone Corporation
	OSDE Organización de Servicios Directos Empresarios
	Palantir Technologies, Inc.
	PricewaterhouseCoopers
	Superintendencia de Telecomunicaciones (Supertel)
	Symantec Corporation
	Team Cymru, Inc.
	Threatmetrix Inc.
	Trend Micro Inc.
	Trustwave
	Verizon Communications Inc.
	Vodafone Group Plc.
	WISeKey SA

قُدِّمت نتائج الإجابات على الاستبيان في صيغة دراسة مجمعة، وتمثل النتائج جميع الإجابات المتاحة على سؤال محدد، بحسب الإقليم أو بحسب المستوى الإنمائي للبلد. ونتيجة لانخفاض عدد الإجابات المقدمة من أوقيانوسيا؛ فإن المناطق المستخدمة هي: "أوروبا"، "آسيا وأوقيانوسيا"، "الأمريكتين"، و"أفريقا".[1]

توضح معظم الأرقام "نسبة المجيبين" الذين اختاروا خيار جواب معين. وفي الحالات التي تسمح بأكثر من إجابة، تحسب النسبة إما وفقا للعدد الإجمالي للبلدان التي أجابت على السؤال المحدد ("ع") أو وفقا للعدد الإجمالي لإجابات الخيارات المحددة ("ن"). القيمتان "ع"، "ن" (بحسب الحالة) موضحتان في جميع ملاحظات المصدر ذو الأرقام. هذا، حيث تستخدم "ع" باعتبارها أساسا لحساب تلك الأسئلة، وقد يصل مجموع النتائج المقدمة إلى 100 في المائة.

وقد سمحت أسئلة عدة في الاستبيان الخاص بالدراسة، باختيار الإجابات من "القائمة المنسدلة" أو إيضاحات إضافية من نوع "النص الحر". في هذه الحالات، خضعت جميع المعلومات المقدمة في الإجابات أو الإيضاحات الإضافية ذات النص الحر للتحليل، وقد خضعت البيانات للتكويد المناسب، من أجل دمج جميع إجابات

[1] الأقاليم الجغرافية التي حددتها شعبة الإحصاءات في الأمم المتحدة على الرابط: http://unstats.un.org/unsd/methods/m49/m49regin.htm

النصوص الحرة مع إجابات القوائم المنسدلة. وفي بعض الحالات، أدى هذا إلى إضافة فئات إجابات جديدة في أرقام النتائج.

وفي الحالات التي تم فيها اعتماد بيانات كمية قدمها المجيبون على الاستبيان، تم عرض ذلك بشكل متكرر باستخدام بيانات القاسم المشترك، بما في ذلك، بحسب الحالة، الرقم الإجمالي لمستخدمي الإنترنت في أحد البلدان، أو الرقم الإجمالي لموظفي إنفاذ القانون. كما تستفيد بعض الأرقام من التصنيف بحسب مستوى تطور البلد.[1] ومتى جمعت البيانات الكمية، تتوافق القيم المقدمة مع المتوسطات، وذلك مع توضيح الربع الأدنى والربع الأعلى باستخدام الأشرطة الإضافية.

[1] تشمل المصادر المستخدمة: دمج مؤشرات التنمية بالبنك الدولي مع مؤشرات الاتصالات العالمية/تكنولوجيا المعلومات والاتصالات لدى الاتحاد الدولي للاتصالات (عدد مستخدمي الإنترنت، بحسب البلد)، مؤشر التنمية البشرية لدى برنامج الأمم المتحدة الإنمائي (التنمية البشرية)، دراسة الأمم المتحدة الاستقصائية لاتجاهات الجريمة وعمليات نظم العدالة الجنائية (عدد موظفي إنفاذ القانون والعدالة الجنائية، وعدد المخالفات المسجلة والمشتبه فيهم في قضايا القتل والاغتصاب).



مكتب الأمم المتحدة المعني بالمخدرات والجريمة

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

Printed in Austria
V.13-80699—February 2013—300